

# TOOLKIT FOR PROTECTING DIGITAL CONSUMERS

*A Resource for  
G20 Policy Makers*

This toolkit was prepared by the OECD Secretariat at the request of the German G20 Presidency and launched at the G20 Consumer Summit in Buenos Aires on 15-16 May 2018.

It was drafted by staff in the OECD Directorate for Science, Technology and Innovation (STI), working with Richard Bates, consultant to the OECD. The leadership and oversight of Gabriela Ramos, OECD Sherpa, and the OECD Sherpa Office, is gratefully acknowledged. Thanks to Angela Gosmann for her valuable help in formatting the report.

This report is issued under the responsibility of the Secretary-General of the OECD.

The opinions expressed and the arguments employed herein do not necessarily reflect the official views of OECD countries or of the G20.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

© OECD, 2018

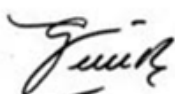
## Preface

The digital shifts underway in the functioning of businesses and markets provide huge opportunities for empowering consumers. As the Internet expands access to goods and services at competitive prices it also brings greater transparency to inform consumer decision making. At the same time, consumer choices in this information-intensive environment are impaired by challenges relating to complexity and uncertainty, sometimes compounded by misleading or fraudulent business practices.

Empowered consumers play an important role in improving economic performance and driving innovation, productivity and competition. Effective consumer protection policies are therefore essential for building trust in the digital economy and enabling everyone to participate fully in it, reaping the opportunities while reducing the risks.

Governments have a key role to play in creating, adapting and maintaining a consumer protection framework that is effective and responsive to the interconnected nature of e-commerce. In 2017, in Düsseldorf, G20 Ministers responsible for the digital economy underlined the importance of consumer protection in their *G20 Roadmap for Digitalisation: Policies for a Digital Future* (the “Roadmap”). In order to support G20 economies in their efforts to implement the Roadmap, and at the request of the 2017 G20 German Presidency, the OECD produced this toolkit and its set of actionable principles.

Building on the long OECD experience in promoting effective consumer protection and in addressing the digital transformation across policy domains, we are pleased to contribute to the international consumer protection agenda with this toolkit, which we hope will be an essential resource for G20 policy makers working to tackle these challenges and support a consumer-driven digital marketplace.



Gabriela Ramos  
OECD Chief of Staff and Sherpa to the G20



Andrew Wyckoff  
Director for Science, Technology and Innovation

## Table of contents

<b>PREFACE .....</b>	<b>3</b>
<b>LIST OF ACRONYMS.....</b>	<b>6</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>1. CONTEXT AND INTRODUCTION .....</b>	<b>11</b>
1.1 An era of dramatic change and new opportunities for consumers .....	11
1.2 About this toolkit .....	13
1.3 What is e-commerce? .....	15
1.4 Key trends in e-commerce .....	17
1.5 Key benefits of e-commerce for consumers .....	19
1.6 Key risks and downsides of e-commerce for consumers.....	20
1.7 E-commerce and consumer trust.....	21
1.8 Consumer protection as a precursor to consumer trust .....	22
<b>2. GENERAL PRINCIPLES .....</b>	<b>23</b>
Introduction .....	23
2.1 Fair business and advertising practices .....	23
2.2 Appropriate disclosures .....	30
2.3 Effective processes for transaction confirmation and payment.....	35
2.4 Measures to address privacy and security risks .....	40
2.5 Product safety across e-commerce supply chains .....	46
2.6 Meaningful access to effective mechanisms to resolve disputes.....	52
<b>3. REGULATORY FRAMEWORK AND INSTITUTIONAL OVERSIGHT .....</b>	<b>57</b>
Introduction .....	57
3.1 Approaches to the regulatory framework .....	57
3.2 Enforcement authorities and their powers .....	60
3.3 Co-operation .....	64
3.4 The policy decision making process.....	72
3.5 Education, awareness and digital consumer competence .....	82
<b>REFERENCES.....</b>	<b>87</b>
<b>NOTES.....</b>	<b>96</b>

## Figures

Figure 1. Rising consumer participation in e-commerce with large cross-country differences .....	17
Figure 2. Popular e-commerce categories in OECD countries .....	19
Figure 3. Preferred means of paying for goods and services online globally .....	37
Figure 4. Individuals having experienced a financial loss from fraudulent online payments in the last three months.....	37
Figure 5. Individuals having experienced privacy violations in the last three months.....	43
Figure 6. Authorities’ investigative powers .....	61
Figure 7. The enforcement pyramid .....	62
Figure 8. Types of enforcement powers .....	63
Figure 9. Types of enforcement actions available to authorities .....	64
Figure 10. Ability to share information with authorities in other countries .....	68
Figure 11. Barriers for international co-operation in consumer protection.....	72
Figure 12. Consumer policy making steps .....	79
Figure 13. Consumer policy tools to target the demand and supply side of markets.....	81

## Tables

Table 1. Share of economies with relevant e-commerce legislation, by region, 2017 (%).....	58
Table 2. Examples of consumer complaint initiatives in G20 economies.....	74

## Boxes

Box 1. High-level general principles.....	23
Box 2. Copycat website fraud .....	25
Box 3. Misleading reference prices: The People of the State of California v. Overstock.com .....	26
Box 4. Enforcement actions on “drip pricing” .....	29
Box 5. Do consumers read online terms and conditions? .....	32
Box 6. Consumer detriment associated with online terms and conditions.....	33
Box 7. The three methods of collecting consumer data.....	41
Box 8. Example of an unsafe product being sold online.....	48
Box 9. Actions undertaken by the ACCC and courts to remove unsafe products from e-commerce	49
Box 10. Online dispute resolution in action.....	56
Box 11. The Competition & Markets Authority and cross-sector co-operation in the United Kingdom .....	65
Box 12. Co-ordinated EU action on social media platforms’ terms and conditions .....	70
Box 13. e-commerce mystery shopping in the European Union .....	76
Box 14. Examples of behavioural biases related to consumer policy.....	78
Box 15. Generic and specific consumer skills.....	83
Box 16. Competences covered by the European Commission’s Digital Competence Framework for Consumers.....	85
Box 17. Example of the description and examples of the knowledge, skills, and attitudes developed for each digital competence .....	86

## List of acronyms

ACCC	Australian Competition & Consumer Commission
ADR	alternative dispute resolution
APEC	Asia Pacific Economic Cooperation
ARP	average reference price
B2B	business to business
B2C	business to consumer
C2B	consumer to business
C2C	consumer to consumer
CIGI	Centre for International Governance Innovation
CMA	Competition & Markets Authority (United Kingdom)
CPC	Consumer Protection Cooperation (European Union)
CPEA	consumer protection enforcement authority
CPSC	Consumer Product Safety Commission (United States)
CRC	Consumer Response Center (United States)
CSCE	Centre de surveillance du commerce électronique (France)
DCT	digital comparison tool
DGCCRF	Direction générale de la concurrence de la consommation et de la répression des fraudes (France)
EC	European Commission
EEA	European Economic Area
EU	European Union
EULA	end user license agreement
FIAGC	Ibero-American Forum of Consumer Protection Agencies
FTC	Federal Trade Commission (United States)
G20	Group of 20
GDP	gross domestic product

ICO	Information Commissioner's Office (United Kingdom)
ICPEN	International Consumer Protection and Enforcement Network
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet service provider
ISR	industry self-regulation
KCA	Korea Consumer Agency
METI	Ministry of Economy, Trade and Industry (Japan)
MOU	Memorandum of Understanding
MSS	mystery shopping survey
ODR	online dispute resolution
OFT	Office of Fair Trading (United Kingdom)
P2P	peer to peer
PPM	peer platform market
PROFECO	Procuraduría Federal del Consumidor (Mexico)
RAPEX	Rapid Alert System for dangerous non-food products (European Union)
SIAR	Inter-American Rapid Alert System
UNCTAD	United Nations Conference on Trade and Development

## Executive Summary

### *The evolving context for digital consumers*

Since its emergence in the 1990s, the character of the commercial Internet has changed dramatically – driving far-reaching changes in society and the economy as a result. Fast-moving digital innovation has transformed the nature of e-commerce and disrupted sector after sector. It has also altered how consumers interact and transact with each other and with the marketplace.

During that quarter-century period, e-commerce has delivered significant benefits and opportunities for consumers. Along with the prospect of achieving better value in a more convenient manner, consumers engaging in e-commerce enjoy much greater choice, including through straightforward access to global markets. There is also an abundance of information concerning the choices that are available, which can translate as greater transparency on price, quality and the reputations of providers. Consumers are able to access a range of digital comparison tools (DCTs) too, helping them navigate and capitalise on – rather than be overwhelmed by – the array of choice and information. Consumers have also gained the means to participate on both the demand and supply sides of the market; and the means to broadcast their experiences of a product or service and its provider to the market. More generally, the progressive lowering of trade barriers, the deepening of global supply chains and the entry of consumers from emerging markets offer significant opportunities to build a truly global, consumer-driven e-commerce marketplace.

However, despite the clear benefits and opportunities offered by e-commerce, the ease and speed with which consumers can engage in online transactions – at anytime, anywhere, and in particular across borders – may create situations that are unfamiliar to them and put their interests at risk. Consumers can be exposed to digital manifestations of risks they have always faced offline, such as fraudulent and deceptive commercial practices, which are a major cause of detriment online; as well as new forms of detriment that are native to the Internet. For example, consumers' understanding of their rights and obligations are often challenged when they make purchases through non-traditional payment mechanisms, such as mobile phone bills; when they acquire digital content products, such as apps or e-books; or when they transact across borders. And in an environment where the scale of a digital platform is proportional to the volume of data it collects about its users, and leverages in its relationship with them, concerns about data use, privacy and security arise. The extent to which hazardous products remain available to purchase online even when/where they have been banned or recalled from the market, is also an ongoing cause for concern, particularly in cross-border contexts.

These risks and challenges can impact consumer trust in digital transactions. Significant numbers of web users still refrain from online purchases because of fears relating to the misuse of personal data and the security of online payments, albeit in the context of an e-commerce ecosystem that now accounts for hundreds of billions of dollars in transactions.

As the G20 seeks to address issues of inclusive growth, equity and fairness in the digital economy, issues relating to consumer trust are moving to the frontlines, especially with the arrival of hundreds of millions of new middle-class consumers from emerging countries. Well-tailored and context-appropriate consumer protections are therefore essential for building the trust needed to further grow and develop e-commerce markets for the economic benefit of consumers and businesses alike; and more effective implementation of consumer rights is essential for e-commerce to reach its full potential.

### *Principles and practices for protecting digital consumers*

This toolkit provides a set of principles and practices for protecting digital consumers and enhancing trust in e-commerce. It is designed to serve as a practical resource for policy makers in G20 economies, which can inform and support their endeavours to create, adapt or maintain a consumer protection framework that is effective in:



- ensuring consumers are empowered to take advantage of the opportunities e-commerce offers, while being adequately protected from the risks it presents
- covering the wide variety of forms that e-commerce now takes, including transactions between consumers, transactions via mobile devices, and transactions that do not involve a monetary payment
- supporting the further growth of competitive e-commerce markets and continued innovation in this respect, for the benefit of consumers and businesses alike.

Beyond policy makers, businesses, civil society, and other stakeholders who engage with and contribute to policy development processes concerning consumer protection in e-commerce may also find the toolkit useful.

While this toolkit has been developed at the request of the German G20 Presidency, its relevance is not confined to G20 economies. Policy makers in any jurisdiction that is seeking to ensure consumers can engage confidently and securely in online transactions, may find it to be a useful resource.

The toolkit consists of three chapters. Chapter 1 provides the context for this toolkit. It offers an overview of the drastic changes in the e-commerce landscape during the last quarter century and of what this has meant for consumers. It then outlines the origins of this toolkit and its intended purpose.

Chapter 2 is organised around six high-level general principles (see below). These principles have been formulated for e-commerce and are derived from – and are common to – the OECD’s *Recommendation on Consumer Protection in E-commerce* (2016 – hereafter the *OECD Recommendation*) and the *United Nations Guidelines for Consumer Protection* (2015 – hereafter the *UN Guidelines*). Taken together, these six principles offer a foundation for policy evaluation and design that G20 economies can utilise in their efforts to protect and empower digital consumers.

In each instance, a statement of the principle describes the underlying objective that the principle seeks to achieve. This is followed by a summary of the relevant provisions in the *OECD Recommendation* and the *UN Guidelines*. The issues to which each principle is addressed are then discussed, with reference to the detriments each issue can cause for consumers, along with examples and relevant data. Good practice examples are then provided, which highlight where consumer protection enforcement authorities (CPEAs) in G20 economies, as well as other agencies, have taken actions that accord with the principle being advocated.

The toolkit’s six high-level general principles are:

- 1. Fair business and advertising practices:** e-commerce businesses should act in accordance with fair business and advertising practices. They should not make any representation that is likely to be deceptive, fraudulent or unfair.
- 2. Appropriate disclosures:** e-commerce businesses should provide clear and accurate disclosures about themselves, the goods or services offered, and the transaction conditions, so that consumers have information sufficient to make an informed decision about a transaction.
- 3. Effective processes for transaction confirmation and payment:** e-commerce businesses should not process a transaction unless the consumer has given express consent and should provide easy-to-use payment mechanisms with appropriate limitations on consumer liability for unauthorised uses.
- 4. Measures to address privacy and security risks:** e-commerce business practices regarding consumer data should be lawful, transparent and fair, enable consumer participation and choice, and include reasonable security safeguards.
- 5. Product safety across e-commerce supply chains:** e-commerce businesses should not offer or advertise goods or services that pose an unreasonable risk to the health or safety of consumers; and should co-operate with competent authorities to address such risks.

- 6. Meaningful access to effective mechanisms to resolve disputes:** consumers should be provided with meaningful access to fair and easy-to-use mechanisms to resolve disputes and obtain redress without undue cost or burden.

Chapter 3 focuses on the regulatory framework and institutional oversight that is required to put the high-level general principles into practice. The starting point for policy makers engaging in this endeavour is to review existing frameworks and then adapt or adopt laws and regulations, to ensure they are cognisant of and responsive to the risks, challenges and opportunities that e-commerce presents for consumers. At the same time, governments need to establish consumer protection authorities capable of overseeing and enforcing these rules, and ensure they are equipped with the necessary legal authority and resources to do so.

Chapter 3 also covers the policy decision making process, including the need to build a robust evidence base and key techniques for doing so – including the important role that behavioural insights can play in this respect. The essential roles that education and digital competence play in empowering consumers to better protect and advance their own interests online, and to achieve better outcomes from e-commerce, are also discussed.

Although effective consumer protection is necessary for establishing a robust e-commerce marketplace, it is not sufficient on its own. Also needed are measures to promote affordable access to broadband connectivity, expand infrastructure, improve digital skills and create incentives for continued innovation, competition and investment in digital business models. G20 consumer protection agencies will therefore have to collaborate with colleagues in other policy areas and across borders to create an inclusive, sustainable future for digital consumers.

# 1. Context and introduction

## 1.1 An era of dramatic change and new opportunities for consumers

A transformation in the business-to-consumer (B2C) relationship began in the 1990s, with the emergence of e-commerce transactions over the Internet. The first ever secure online transaction was completed in 1994 (Grothaus, 2015). This was the era of Web 1.0, where websites served up static content and e-commerce, in its initial incarnation, looked and felt to the consumer like an on-screen version of catalogue shopping. Even so, the range of items available to purchase online was increasing rapidly, and a growing number of consumers were looking to realise the convenience, choice and value that e-commerce promised. In 1999, OECD countries developed the first international “best practices” instrument to address online consumer protection (OECD, 1999a<sup>1</sup>). This provided guidance to a wide range of countries, businesses, self-regulatory organisations and consumer organisations on transposing basic consumer protections to the new, online environment. At that point it was expected that worldwide, roughly one in seven Internet users would be involved in shopping online (OECD, 1999b), spending between USD 20 billion and USD 40 billion (OECD, 2001).

By the time the OECD’s *Recommendation on Consumer Protection in E-commerce* (a revision of the 1999 guidelines) was published in 2016 (OECD, 2016a), the character of the Internet had changed dramatically, driving far-reaching changes in society and the economy as a result. Fast-moving digital innovation had transformed the nature of e-commerce and disrupted sector after sector. It had also altered how consumers interact and transact with each other and with the marketplace; and with the rise of digital content, had changed how people consume certain product categories – e.g. watching films via a streaming service, rather than through a cable television subscription.

The period since 1999 has also witnessed massive growth across G20 economies in the numbers of consumers engaging in e-commerce, the frequency of transactions and the value of e-commerce sales. The billions of dollars of revenue generated by e-commerce in 1999 has since grown to trillions. In some sectors (e.g. the music industry) online sales now account for the majority of revenues.

After moving beyond its origins as a digital channel for the retail of durable goods, e-commerce now covers digital media (e.g. Kobo e-books), the spectrum of services (e.g. Expedia in travel, Zopa in financial services) and perishable goods (e.g. supermarkets, such as Tesco in the United Kingdom, enabling consumers to order groceries online for home delivery).

But it's no longer just the most developed economies that are leading this change. By 2013, the People’s Republic of China (hereafter “China”) had become the largest B2C market in the world, both by number of buyers and overall revenues (UNCTAD, 2015). In Indonesia, where almost 9 in 10 online users have a social media account, social media is becoming an important channel for e-commerce, (UNCTAD, 2015). A key driver of these trends is the use of mobile devices: Indian companies Snapdeal and Flipcart are estimated to receive up to 70% of their orders via mobile phones (Meeker, 2015).

As a result, consumers are now able to fulfil a significant proportion of their product and service needs, no matter how niche, through e-commerce channels. With few exceptions, if the product or service is available in the physical world, it is now available online too. Some services, such as virtual banks, exist only on the Internet and for various media categories (e.g. video, music, the published word, video games and software), the Internet is becoming the dominant delivery channel, as content migrates away from tangible formats.

In some instances, consumers are choosing access to a product over ownership (e.g. streaming music via Spotify, rather than purchasing physical formats). However, for some products and services, licencing agreements between the provider and the consumer can mean boundaries between access and ownership are less clear-cut than was the case in the pre-digital era (see Section 2.2.2.).

As the first medium capable of supporting “many-to-many” communication at scale (Shirky, 2009), the Internet has enabled consumers to interact and transact with their peers on an unprecedented scale. In gaining this capability, consumers can become active participants in the marketplace and in a media of the masses - rather than the passive recipients that characterised the industrial era and mass media. For example, consumers are now able to participate on either the demand or supply side of markets by using peer platform providers (e.g. eBay, DiDi, Airbnb) that leverage the many-to-many capability of the Internet to aggregate and instantaneously match supply and demand at massive scale. As a result, consumers can bypass conventional providers completely in some sectors and buy, sell, rent, swap, share, barter, lend and exchange goods and services to/from/with each other, in ways that were not feasible in the pre-digital economy. This many-to-many capability also underpins ratings and review platforms and social media, which have given consumers a voice in the marketplace and the means to share their experiences widely.

The channels through which online transactions are mediated have also evolved, as innovative technologies have emerged and been rapidly embraced by consumers. Most notable among these is the smartphone, a device that was still eight years away in 1999. These have made the Internet mobile and granted access to it to hundreds of millions of people globally. Smartphones have also given rise to a constellation of e-commerce focused software applications (apps) and ignited e-commerce in countries such as India and China, with a distinct subset of e-commerce, mobile commerce (“m-Commerce”), emerging as a result.

Nominally free-to-use services, such as social media and online search, have become bedrocks of consumers’ online activity and key features in the e-commerce landscape. By providing tools that enable businesses to tailor and micro-target advertisements at specific consumer segments, these platforms also play an instrumental role for actors on the supply side of markets. These tools leverage the granular data that social media platforms and search engines capture or infer about their users, including demographic details, user locations, preferences, search histories, social networks, contacts and prior purchases.

In the Internet of Things (IoT), smart home devices and appliances can also serve as portals to online commerce. Some promise consumers even greater convenience and reduced friction when placing orders manually (e.g. voice-controlled transactions via Amazon’s virtual assistant, Alexa, which inhabits its Echo smart speaker), while other devices and appliances can re-order their own consumables autonomously (e.g. the smart washing machine that detects detergent levels and re-orders new supplies as they run low). But again, as with social media and search, the functionality of some IoT devices can be dependent on the large-scale collection of consumer data. The consequences of extensive user data collection are outlined below and addressed in greater detail in Section 2.4.

Payment systems that are native to the Internet have grown to become key players in the e-commerce landscape (e.g. PayPal, Alipay) and can help assuage consumer fears about transacting online. These payment innovations represent early success stories in what is now a rapidly growing FinTech ecosystem – where banks are virtual, loans and foreign currency exchange are brokered online (and, in some cases, between peers), and the “crowd” can fund the development of new products it would like to see come to market.

It is worth noting the inter-play that can exist between and across these innovations and the platforms they give rise to. For example, WeChat in China is a smartphone app that integrates a social media platform, a payment system and e-commerce portals (Chao, 2017).

The evolution outlined above has partly been made possible by continued improvements in consumer access to broadband Internet. These have led to greater coverage, speed and affordability. As noted above, the smartphone has also made the Internet mobile and, as a result, accessible to a considerable proportion of the global population. In combination with the progressive lowering of trade barriers, the expansion and deepening of global supply chains and, perhaps most importantly, the entry of consumers from emerging markets, these

developments have opened up significant opportunities to build a truly global, consumer-driven e-commerce marketplace (OECD, 2017b).

### 1.1.1 A changed world brings new challenges

However, despite the clear benefits and opportunities offered by e-commerce, the ease and speed with which consumers can engage in online transactions – at anytime, anywhere, and in particular across borders – may create situations that are unfamiliar to them and put their interests at risk (OECD, 2016a). With the increasing complexity of the online environment and the emergence of new e-commerce business models, the benefits may be accompanied by actual or potential risks and challenges. For example, consumers’ understanding of their rights and obligations are often challenged when they make purchases through non-traditional payment mechanisms, such as mobile phone bills or pre-paid cards; when they acquire digital content products, such as apps or e-books; or when they transact across borders.

Risks and challenges also include digital manifestations of risks consumers have always faced offline, such as fraudulent and deceptive commercial practices, which have become a major cause of consumer detriment online. In addition, consumers also face forms of detriment that are native to the Internet, such as online identity theft (OECD, 2017b).

In an environment where the scale of a digital platform is proportional to the volume of data it can collect about its users and leverage in its relationship with them, concerns about data use, privacy and security also arise (see Section 2.4). In some respects, these platforms have helped erode traditional information asymmetries. For example, a search engine or digital intermediary can assist consumers in comparing the price and reputation of a wide range of prospective providers for a good or service they are seeking, in ways and with a level of convenience that would not be possible if these platforms did not exist. However, at the same time, platforms’ data gathering practices can fuel what one Silicon Valley analyst has described as an “extreme information asymmetry” (Lanier, 2013), where the consumer is rendered transparent to the platform, yet the platform’s practices remain opaque to the consumer. In addition, platforms leverage algorithms fed by these data to shape consumers’ experiences of their services, including what consumers can and cannot see. Data-fed algorithms also have the capacity, in theory at least, to determine the prices that individual consumers are quoted (Mohammed, 2017). The lack of a means to opt out of, or turn off these functions leaves consumers facing a “take it or leave it” choice when using these platforms.

Well-tailored and context-appropriate consumer protections and competitive markets are therefore essential to build the trust needed to further develop these markets for the benefit of consumers and businesses alike; and more effective implementation of consumer rights is essential for e-commerce to reach its full potential. As outlined in the following section, well-tailored consumer protections and the type of regulatory framework required to give effect to these are very much the focus of this toolkit.

## 1.2 About this toolkit

### 1.2.1 Origin of this toolkit

The Ministerial Declaration (G20, 2017) that followed the April 2017 G20 Digital Economy Ministerial Conference in Düsseldorf, Germany, emphasised the importance of consumer protection in the digital economy, stating that:

*G20 countries continue to address a number of consumer challenges to ensure that online businesses provide consumers with information sufficient to make informed decisions, for example through consumer information that is easy to understand. Consumers also need to be empowered to take control of their online identity. (G20, 2017)*

In the Roadmap that was annexed to the Declaration, G20 Ministers noted the great importance of consumer protection. They also agreed to further study new business models in relation to consumer trust and to continue the discussion on how to protect consumers in the digital economy under the Argentinian presidency. The Declaration also noted the first ever G20 Consumer Summit,<sup>2</sup> held on 15 March 2017 in Berlin.

At the Consumer Summit, Consumers International and Verbraucherzentrale Bundesverband<sup>3</sup> presented recommendations on behalf of the worldwide consumer movement (Consumers International & VZBV, 2017). Among other things, these recommendations called on the G20 to recognise the importance of consumer trust and empowerment in realising the benefits of the digital economy; and requested that the OECD develop “a toolbox of policies, actions and measurement criteria” (Consumers International & VZBV, 2017).

### 1.2.2 Purpose of this toolkit

This toolkit sets out principles and practices for protecting digital consumers and enhancing trust in e-commerce. It is designed to serve as a practical resource for policy makers, which can inform and support them in their endeavours to create, adapt or maintain a consumer protection framework that is effective in:

- ensuring consumers are empowered to take advantage of the opportunities e-commerce offers, while being adequately protected from the risks it presents
- covering the wide variety of forms that e-commerce now takes, including transactions that take place between consumers, via mobile devices, and without monetary payment
- supporting the further growth of competitive e-commerce markets and continued innovation in this respect, for the benefit of consumers and businesses alike.

Beyond policy makers, businesses, civil society, and other stakeholders who engage with and contribute to policy development processes concerning consumer protection in e-commerce, may also find the toolkit useful.

While this toolkit has been developed at the request of the German G20 Presidency, its relevance is not confined to G20 economies – policy makers in any jurisdiction that is seeking to ensure consumers can engage confidently and securely with e-commerce may find it to be a useful resource.

### 1.2.3 Structure and scope of this toolkit

The remainder of this chapter summarises the characteristics of e-commerce, as well as key trends in e-commerce growth, the benefits that consumers can enjoy, the risks and downsides they can experience, the importance of consumer trust, and the role of consumer protection in engendering that trust.

Chapter 2 is organised around the six general principles set out below. The principles have been formulated for e-commerce and are derived from – and are common to – the *Recommendation on Consumer Protection in E-commerce: OECD Recommendation* (OECD, 2016a) (hereafter the *OECD Recommendation*) and the *United Nations Guidelines for Consumer Protection* (United Nations, 2015) (hereafter the *UN Guidelines*).

The six principles relate to:

1. fair business and advertising practices
2. appropriate disclosures
3. effective processes for transaction confirmation and payment
4. measures to address privacy and security risks
5. measures to address product safety risks across e-commerce supply chains
6. meaningful access to effective mechanisms to resolve disputes.

In each instance, a statement of the principle describes the underlying objective it seeks to achieve. This is followed by an overview of the relevant provisions in the OECD *Recommendation* and the *UN Guidelines*. The issues to which each principle is addressed are then discussed, with reference to the detriments these can cause for consumers, along with examples and relevant data. Good practice examples are then provided, highlighting where CPEAs in G20 economies, as well as other agencies, have taken actions relevant to the principle being advocated.

Chapter 3 focuses on the regulatory framework and institutional oversight that is required in order to put the general principles presented in Chapter 2 into practice; and to then uphold them. Section 3.1 draws on analysis by the OECD and by the United Nations Conference on Trade and Development (UNCTAD) to provide a snapshot of how different countries and regions have approached this. It also examines the potential that self-regulation offers in relation to protecting digital consumers.

Consumer protection enforcement authorities are the focus of Section 3.2, which discusses the expertise and powers, including sanctions, CPEAs require in order to intervene in the marketplace and protect and empower digital consumers. It also outlines how authorities can utilise their powers most effectively. Section 3.3 discusses the challenges that the rapidly evolving digital marketplace can pose for CPEAs and, as a result, the need for enhanced co-operation. It looks first at the need for domestic authorities to co-operate in a cross-disciplinary manner, recognising that contemporary consumer protection challenges increasingly occur at the points where traditional regulatory mandates – i.e. for consumer protection, competition, data protection and specific sectors – intersect. It then turns to the need for cross-border co-operation between authorities, at both the regional and global levels, given that risks to consumers – whether from unsafe products or fraudulent practices – can quickly traverse borders in the increasingly global marketplace.

The policy decision making process is the focus of Section 3.4, which discusses the need to build a robust evidence base and key techniques for doing so, including the important role that behavioural insights can play in this respect. A six-step guide to developing consumer policy – adapted from the OECD's 2010 *Consumer Policy Toolkit* (OECD, 2010a) – is then presented. The six-step process provides policy makers with a framework for developing policy interventions that are evidenced-based and well designed; and can help them determine whether and how they should intervene in a market to address a specific consumer issue.

The concluding section (3.5) is dedicated to consumer education and digital competence. It highlights the key roles these can play in empowering consumers to better protect and advance their own interests when navigating the online environment, and to achieve better outcomes from e-commerce.

In terms of scope, the toolkit is oriented to the powers and responsibilities of consumer protection authorities and does not address the full range of policy areas relevant to ensuring the success of e-commerce markets for consumers. For example, issues related to access, inclusion and competition are not covered here; and privacy and digital security risks are not addressed in depth. However, a number of these issues are covered by other G20 related work by the OECD.<sup>4</sup>

### 1.3 What is e-commerce?

The OECD has defined e-commerce in the following terms:

*An e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online.* (OECD, 2011)



A broader perspective – reflective of the evolution of e-commerce outlined above – informed revisions to the OECD *Recommendation* in 2016 (OECD, 2016a), resulting in its recognition of key developments in the e-commerce landscape, namely:

- the growth of non-monetary transactions (i.e. in consumers' usage of services that are nominally free to use, such as social media and search engines)
- the growing uptake of digital content products (i.e. media that is downloaded or streamed)
- the advent of active consumers who participate in the creation and provision of products and services; and in shaping the reputations of products, services and their providers
- the growing proportion of e-commerce transactions that are undertaken using mobile devices (sometimes referred to as m-commerce)
- the fundamental role that consumer data plays in e-commerce and the elevated privacy and security risks that arise as a result.

E-commerce can take place on a business-to-business (B2B) basis, a business-to-consumer (B2C) basis, or a consumer-to-consumer/peer-to-peer (C2C, P2P) basis (i.e. via peer platform marketplaces in what is sometimes referred to as the “sharing” or “collaborative” economy). The two consumer-centric forms of e-commerce (B2C and C2C) form the focus of this toolkit, primarily from the perspective of the consumer as the purchaser or user of goods and services, rather than as the creator or provider of them.

### 1.3.1 *The distinct characteristics of e-commerce*

This toolkit often refers to the distinct characteristics of e-commerce and the influence these can have on consumer behaviour. Compared to transactions undertaken via offline channels (e.g. brick-and-mortar stores), the traits that can set e-commerce transactions apart are:

- the remote coordination and processing of transactions (in common with other distance selling channels), which typically occur at a distance and, in some instances across borders, even if the service itself is delivered in-person
- the absence, generally speaking, of an opportunity to inspect, test or evaluate a product or service prior to the initial transaction (again, in common with other distance selling channels). Exceptions can include “showrooming”, whereby consumers inspect an item in a brick-and-mortar store prior to purchasing online (potentially from a different provider at lower cost); and free trials associated with digital content
- the more impersonal<sup>5</sup> experience, given that transactions are conducted through screens; and, to the extent that interactions with vendors' sales staff or customer service representatives exist, these are via remote channels, rather than face-to-face, and may involve artificial intelligence
- in many instances, the need for the user to create and manage an account and, as a result, agree to platforms' terms of use; and to input payment details in order to complete a transaction, if a purchase is being made
- the amount and types of data that providers gather about consumers during the course of a transaction; and providers' usage of these data thereafter.

These characteristics can – individually or in combination – influence the degree to which a consumer is trusting of online providers and e-commerce processes and, as a result, their willingness to undertake transactions online.



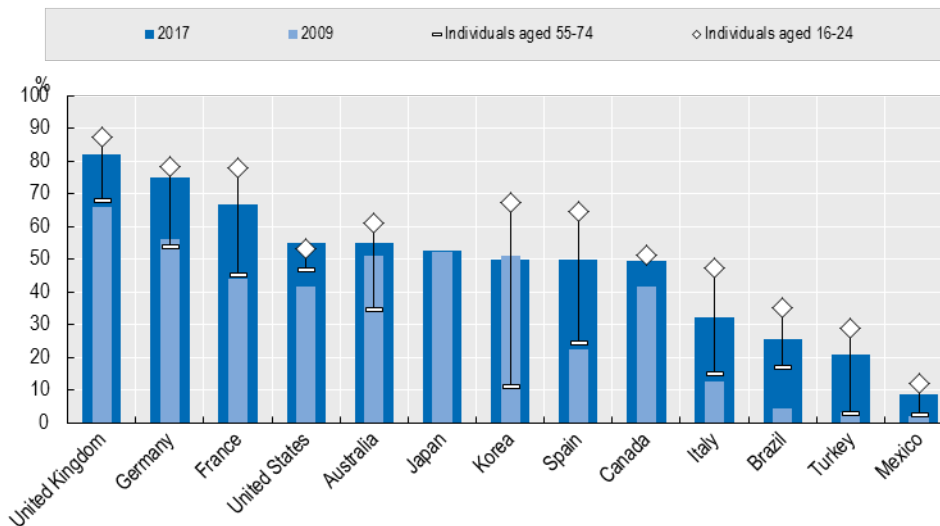
## 1.4 Key trends in e-commerce

### 1.4.1 Growth in consumer take-up of e-commerce

Data for OECD countries shows the proportion of individuals who made an online purchase in 2017 was 52.7%, up from 33.6% in 2009. For the OECD countries that are G20 economies, that figure is lowest in Mexico (8.8%) and highest in the United Kingdom (82%) (Figure 1). There is wide variation across age groups, with 16 to 24-year olds (63.5%) being twice as likely as consumers aged 55 to 74 (31.5%) to have purchased a good or a service online during the past 12 months (OECD, forthcoming).

In the European Union (EU), the proportion of the EU population that has bought online in the previous 12 months has almost doubled during the last decade – growing from 30% in 2007 to 57% in 2017. For Internet users in the European Union, that figure rises to 68% (Eurostat, 2017).

**Figure 1.** Rising consumer participation in e-commerce with large cross-country differences  
2009-17, OECD countries



Source: OECD (forthcoming), “A dynamic e-commerce landscape: Developments, trends and business models”; OECD (2018d), *ICT Access and Usage by Households and Individuals* (database), <http://oe.cd/hhind> (accessed April 2018).

### 1.4.2 Growth in consumer e-commerce revenues

UNCTAD estimates that global B2C e-commerce was worth USD 2.9 trillion in 2015. China, which is now the world’s largest market for B2C e-commerce, both by number of online buyers and revenue, accounted for USD 617 billion of that total. The United States was close behind, with revenues of USD 612 billion (UNCTAD, 2017b; UNCTAD, 2015). Together these two countries account for around 42% of the global B2C e-commerce market. Market intelligence firm, eMarketer, forecasts that worldwide sales will hit USD 4.5 trillion by 2021 (eMarketer, 2017).

With regards to the regional share of the global e-commerce market, analysis by the E-commerce Foundation (an e-commerce trade body) indicates that the Asia-Pacific region accounts for the largest share of global e-commerce (at 46.5%), followed by North America (28.3%), Europe (22.2%), Latin America (1.5%), the Middle East & North Africa (1.1%) and other countries (0.4%) (E-commerce Foundation, 2016).

### 1.4.3 Growth in e-commerce as a proportion of all B2C sales

Although B2C e-commerce currently represents a small proportion of overall retail sales, its growth rate surpasses that of offline retail. eMarketer estimates that e-commerce (excluding travel and event tickets) represented 10% of total retail sales in 2017 and forecasts that figure will surpass 16% by 2021 (eMarketer, 2017). In OECD countries, B2C e-commerce has grown continuously and at a faster rate than overall retail sales (OECD, 2017a). The latest available data for the United States (for Q3, 2017) shows that while e-commerce accounted for only 9.1% of all retail sales in the period, it had grown 15.5% year-on-year, compared to 4.3% for retail sales overall (US Department of Commerce, 2018).

### 1.4.4 Cross-border purchases

While only limited data is available on consumer engagement in cross-border e-commerce, EU survey findings offer some insight on the extent to which this is happening. Eurostat data for 2017 shows that, of consumers who had made online purchases in the 12 months prior to the survey, 33% had bought from sellers in other EU countries (up from 25% in 2012); and 23% had bought from sellers outside the European Union (up from 13% in 2012).

Of those consumers who had made a cross-border purchase, 80% had bought or ordered physical goods such as electronics, clothes, toys, food, groceries, books and CDs/DVDs. Lower proportions had made cross-border purchases of travel, accommodation or holiday arrangements (34%), or products that are downloaded or accessed from websites or apps (25%) (Eurostat, 2017).

### 1.4.5 The growth of mobile commerce

M-commerce refers to the subset of e-commerce that consumers conduct through mobile devices, primarily smartphones and tablets. eMarketer forecasts that by 2021 worldwide mobile commerce (excluding travel and event tickets) will be worth USD 3.6 trillion and account for 73% of B2C e-commerce, compared to 52.4% in 2016 (eMarketer, 2018). In India, platforms such as Snapdeal and Flipcart are estimated to receive up to 70% of their orders via mobile phones (Meeker, 2015).

With regards to the proportion of consumers making purchases through mobile devices, just over half of consumers in the United States have ever made an online purchase using a mobile (Smith and Anderson, 2016). Across the European Union, 59% of online shoppers had used a smartphone and 52% had used a tablet to make an online purchase in the previous 12 months (European Commission, 2015e).

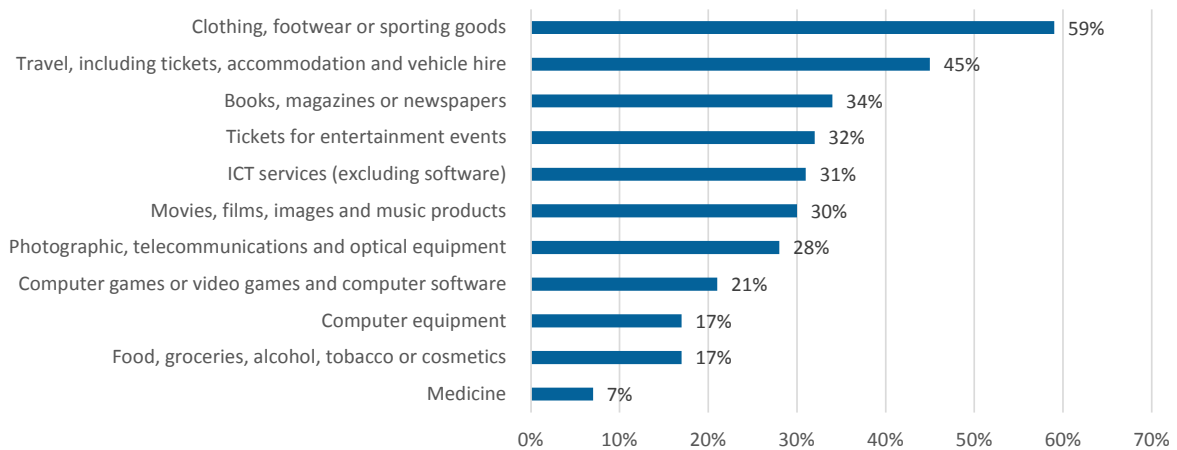
### 1.4.6 What do consumers buy online?

Data for OECD countries indicates that clothing, footwear and sporting goods was the most popular category for e-commerce purchases in 2017. Fifty-nine percent of all consumers who had engaged in e-commerce had made a purchase in this category. This was followed by products and services relating to travel (45%); books, magazines and newspapers (34%); and tickets for entertainment events (32%) (Figure 2).

However, the averages for each category mask notable variations between countries. For example, tickets for entertainment events were purchased by only 6% of consumers buying online in Canada; and clothing, footwear and sporting goods were much more popular in Korea (at 87%).

**Figure 2.** Popular e-commerce categories in OECD countries

As a percentage of all consumers who purchased online in 2017



Source: OECD (forthcoming), "A dynamic e-commerce landscape: Developments, trends and business models".

#### 1.4.7 Social media and e-commerce

Analysis by WE ARE SOCIAL (a digital agency) indicates that 42% of the global population (3.2 billion people) are now social media users (Kemp, 2018). As an arena where consumers can seek out the perspectives and recommendations of peers, and are exposed to micro-targeted brand advertising, social media can form an important part of the purchasing journey online. In Indonesia, where the number of active social media users (130 million [Kemp, 2018]) has almost reached parity with the number of Internet users (133 million), it serves as an important channel for e-commerce, particularly for smaller businesses (UNCTAD, 2015). In the United States, 15% of consumers made a purchase after following a link from a social media site (Smith and Anderson, 2016).

#### 1.5 Key benefits of e-commerce for consumers

For consumers who have the means to do so, engaging in e-commerce can open up a range of benefits and opportunities, which are summarised in the following:

**Greater choice:** e-commerce offers consumers greatly enhanced choice. For example, Amazon.com carries more than 12 million items (360pi, 2016), rising to 562 million when its Marketplace listings are included (scrapehero.com, 2018). By comparison, a Walmart Supercenter carries an average of 142 000 items (Walmart, n.d.). E-commerce also brings the global marketplace to consumers' fingertips, providing them with the means to buy across borders in a much more straightforward way than was previously possible.

**Greater convenience:** e-commerce lowers transaction costs and empowers consumers to engage with the market in an efficient manner, at the time and place of their choosing, rather than being bound by providers' business hours and locations. Innovative technologies such as virtual personal assistants with voice ordering capabilities may enhance this convenience further.

**Better value:** continuous innovation, the economies of scale that successful platforms achieve, the lower overheads that online providers enjoy (Wigglesworth, 2017) and, in some markets, stronger competition resulting from low switching costs (given competitors are only a click away), can translate as cost savings and free-to-use services for consumers. It has been estimated that savings from online shopping amount to EUR 11.7 billion in the European Union, equivalent to 0.12% of the European Union's GDP (European Commission, 2013a). The 2017 Ipsos Global Trends survey, which included all 19 G20 economies, found that globally, 71% of consumers agreed with the statement: "I can find better deals shopping online than shopping in traditional stores" (Ipsos, 2017).

**More information, greater transparency:** the Internet grants easy access to an abundance of information concerning the quality and pricing of products and services, and the reputations of their providers. It therefore supports greater transparency than was possible in the pre-Internet era, enabling more effective comparisons and better-informed decision making for consumers (more so when consumers use digital comparison tools to navigate this information – see below). However, these benefits are tempered by the risks of information overload and the challenges inherent in identifying reliable and impartial sources. And, as Section 1.1 noted, while greater market transparency can help erode traditional information asymmetries, this benefit can be countered by new forms of information asymmetry that may arise from online platforms’ data gathering and usage practices.

**Access to digital comparison tools:** the Internet has given consumers access to a range of DCTs and aggregation and intermediary platforms that can filter, parse and curate market information, and can do so in accordance with preferences and parameters set by the consumer. Where they function well, these services can serve to lower transaction costs and deliver better deals, by enabling consumers to conveniently and efficiently compare and choose between offers from across the market. They can also be seen by suppliers as an efficient way to reach large numbers of consumers and the price transparency they create can increase competition among suppliers and reduce prices (OFT, 2013). A 2011 survey undertaken for the European Commission found that DCTs provide average savings of 7.8% on the online retail price across Europe (Civic Consulting, 2011). However, the practices of some DCTs can be problematic (see below and section 2.1).

**The opportunity to be a more active market participant:** as noted at Section 1.1, peer platform providers such as eBay and Airbnb have made it much easier for consumers to participate on both the demand and supply sides of the market. Similarly, social media and review and ratings systems have given consumers a voice with which they can engage directly and publicly with a provider and easily share their experiences of a product or service – whether positive or negative – with the provider and with each other.

### 1.6 Key risks and downsides of e-commerce for consumers

The general principles that form the basis of Chapter 2 seek to address the risks and downsides that consumers can face when engaging in e-commerce and the detriment that can arise from these. Each principle is accompanied by an “overview of the issue” section, which highlights the risks and challenges that the principle seeks to address. These overviews are summarised below.

**Unfair business and advertising practices:** consumers can be deceived as to the nature of the product or service (or of the advertising itself) and subjected to aggressive and/or misleading marketing and pricing techniques (e.g. drip pricing). Fraudulent operators can imitate legitimate websites and manipulate search engine results in order to exploit consumers. Businesses might also falsely represent themselves as consumers and post reviews or endorsements that inflate their own reputations or denigrate those of competitors. Operators of DCTs may seek to promote the offers of firms with whom they have commercial relationships, rather than the offers that represent the best value for the consumer.

**Problems relating to disclosure and the nature of online terms and conditions:** if online terms and conditions are long and complex, or hidden in a website or app, consumers may face high search costs, or find themselves locked in or otherwise committed to contracts they would not knowingly have agreed to. They might also find themselves in receipt of goods or services that either do not meet their needs, are of a lower quality than expected, or, in the case of some digital content products, cannot be used in the way the consumer reasonably expects. If privacy notices and other terms of use are either misleading or unintelligible to the reader, consumers may unwittingly agree to personal data being collected, used and shared in ways they would not knowingly approve of. The absence of effective disclosure can also reinforce information asymmetries.

**Problems relating to payments and transaction confirmation:** without adequate payment security, transaction data provided in the context of e-commerce payments could be lost, stolen or otherwise misused. Unless adequate minimum protections are in place and apply regardless of payment method, consumers could be exposed to potentially severe financial losses resulting from cybercriminal activity.

If effective transaction confirmations are lacking, consumers could be left liable for charges for purchases they have not authorised (e.g. if a child makes an in-app or in-game purchase unbeknown to its parent, when using the parent's device). Conversely, in some instances consumers may be under the impression they have completed an intended purchase when in fact the transaction failed.

**Issues relating to data and privacy:** as noted at Section 1.1, the extensive collection of consumer data by online platforms can feed powerful new forms of information asymmetry. Platforms can leverage algorithms fed by these data to shape and otherwise manipulate consumers' experiences of their services, including what consumers can and cannot see. The same capabilities could also give platforms the means to personalise prices, although the extent to which this is happening remains unclear. The increased prevalence of large-scale data breaches underlines the need for effective security measures, if consumers' privacy, financial interests and wider safety are to be adequately protected.

**The continued availability of unsafe products in e-commerce:** a key issue affecting consumer trust in e-commerce, especially as it relates to cross-border transactions, is the number of unsafe products that are available for sale online. As the OECD's international product safety sweep in 2015 highlighted, unsafe products that have been prohibited from sale or recalled from the market, remain available through e-commerce channels in several countries. Of the nearly 700 products inspected for the purpose of detecting banned or recalled products during the OECD sweep, 68% were available for sale online.

As Section 2.6 highlights, **dispute resolution and redress mechanisms that are both effective and accessible, are vital** for helping consumers to resolve problems and rectify detriments that result from the above risks. The absence of such mechanisms can act as a barrier to consumers engaging with e-commerce and, if coupled with unresolved negative experiences, can lead consumers to disengage.

### 1.7 E-commerce and consumer trust

For e-commerce to continue to grow and generate economic benefits for consumers and supply side actors alike, consumers need to be able to trust digital markets (UNCTAD, 2017a). High levels of consumer trust stimulate online purchase intentions and support customer retention, while low levels are the primary reason individuals refrain from shopping online (Gefen and Straub, 2004).

Data from the Centre for International Governance Innovation's (CIGI) Global Survey on Internet Security<sup>6</sup> show that 22% of respondents (all of whom were Internet users) never buy goods or services online. Within that segment, 49% cited not trusting online shopping as the key reason, although that figure varied widely across the 24 countries surveyed. Within the 16 G20 economies featured, it was highest in Turkey (54%), and at or above 50% in Australia (50%), Mexico and South Africa (both at 51%). The figure was lowest in China (18%) and Japan (25%) (CIGI, 2017).

Significant numbers of web users still refrain from online purchases because of fears relating to the misuse of personal data, and the security of online payments (OECD, 2017). Indeed, the CIGI survey found that 55% of respondents were more concerned about their online privacy than a year ago. Among that segment, 82% cited cyber criminals as contributing to their increased concern, and 74% cited Internet companies (CIGI, 2017).

The critical role that trust plays in the development of online markets has long been recognised by international institutions. For example, the OECD first called for the development of consumer protection guidelines to enhance trust in e-commerce in a 1998 Declaration (OECD, 1998), which resulted in the 1999

OECD *Guidelines on Consumer Protection in the Context of Ecommerce* (OECD, 1999a). A more recent Declaration, an outcome of the OECD's 2016 Digital Economy Ministerial Meeting in Cancún (OECD, 2016d), saw ministers commit to reduce impediments to e-commerce within and across borders with policies that strengthen consumer trust and product safety. Signatories to the Declaration included OECD countries and Argentina and Indonesia (OECD, 2016d). UNCTAD's Programme on E-commerce and Law Reform has been supporting developing countries in Africa, Asia and Latin America, in their efforts to establish legal regimes that address issues raised by e-commerce and build trust in online transactions (UNCTAD, 2017a). UNCTAD also delivers various technical co-operation and capacity building programmes in support of these objectives.

### **1.8 Consumer protection as a precursor to consumer trust**

There is a need for governments to ensure that consumer protection frameworks are cognisant of, and offer an adequate and effective response to, the risks, challenges and opportunities that contemporary forms of e-commerce present for consumers. Doing so can play a vital role in enhancing consumer trust and consumers' capacity to participate in domestic and cross-border e-commerce in a safe and informed manner. Effective consumer protection can also help reduce differences between the well-informed and the less-well-informed, the protected and the unprotected, and, ultimately, the haves and the have-nots (OECD, 2017b). This need provided some of the impetus for the revisions of the *UN Guidelines* (in 2015) and the *OECD Recommendation* (in 2016). Notably, the revised *UN Guidelines* now contain guidance specific to e-commerce (UNCTAD, 2017a).

Findings from the 2017 CIGI global survey highlight how consumer protection can serve as a precursor to trust. Of respondents who buy online at least once a month, almost all (94%) view consumer protection online and its component dimensions, such as protection of data privacy (also 94%) and protection against cybercrime (also 94%), as important in determining whether they will engage in online shopping (CIGI, 2017).

However, UNCTAD's global mapping of e-commerce-specific consumer protection legislation indicates considerable scope for progress in this respect. It found that e-commerce protection is far from the norm, with only "patchy" coverage and significant gaps in many developing and transition countries (UNCTAD, 2015).

## 2. General principles

### Introduction

International consensus has emerged around a set of recommended practices that businesses should follow when engaging in transactions, including non-monetary transactions, with consumers online; or when facilitating these on behalf of consumers. These recommended practices have been organised here into a set of six high-level general principles (Box 1). These six principles offer a foundation for policy evaluation and design that G20 economies can utilise in their efforts to protect and empower digital consumers.

This chapter presents the six principles in turn. In each instance, the relevant sections of key international instruments – primarily the *OECD Recommendation* (OECD, 2016a) and the *UN Guidelines* (United Nations, 2015) – are summarised. A discussion of the key consumer issues that each principle seeks to address is then provided, followed by good practice examples.

The subsequent chapter (Chapter 3) then considers the regulatory infrastructure that is required to implement and enforce the six principles.

### BOX 1. HIGH-LEVEL GENERAL PRINCIPLES

- **Fair business and advertising practices:** e-commerce businesses should act in accordance with fair business and advertising practices. They should not make any representation that is likely to be deceptive, fraudulent or unfair.
- **Appropriate disclosures:** e-commerce businesses should provide clear and accurate disclosures about themselves, the goods or services offered, and the transaction conditions, so that consumers have sufficient information to make an informed decision about a transaction.
- **Effective processes for transaction confirmation and payment:** e-commerce businesses should not process a transaction unless the consumer has given express consent and should provide easy-to-use payment mechanisms with appropriate limitations on consumer liability for unauthorised uses.
- **Measures to address privacy and security risks:** e-commerce business practices regarding consumer data should be lawful, transparent and fair, enable consumer participation and choice, and include reasonable security safeguards.
- **Product safety across e-commerce supply chains:** e-commerce businesses should not offer or advertise goods or services that pose an unreasonable risk to the health or safety of consumers; and should co-operate with competent authorities to address such risks.
- **Meaningful access to effective mechanisms to resolve disputes:** consumers should be provided with meaningful access to fair and easy-to-use mechanisms to resolve disputes and obtain redress without undue cost or burden.

### 2.1 Fair business and advertising practices

#### Statement of the principle

E-commerce businesses should act in accordance with fair business and advertising practices. They should not make any representation that is likely to be deceptive, fraudulent or unfair.



### 2.1.1 Summary of the international instruments

#### OECD Recommendation

Part B of the *Recommendation* states that businesses engaged in e-commerce should act in accordance with fair business, advertising and marketing practices. The following summarises the key provisions from Part B, with the number of the relevant provision shown in parentheses:

- Businesses should not engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair (4), including deceptive practices related to the collection and use of consumers' personal data (8).
- Terms and conditions that are likely to affect a consumer's decision regarding a transaction should not be misrepresented nor hidden (5); and should not be unfair (6). They should also allow consumers to withdraw from a confirmed transaction in appropriate circumstances, even where this is not obliged (19); and should be proportionate to the damage likely to be caused, if stipulating monetary remedies for a breach of contract by the consumer (7).
- Express or implied representations concerning adherence to industry self-regulatory codes or programmes, privacy notices or any other policies or practices should be complied with (11).
- Advertising and marketing should: be clearly identifiable as such (13); identify the business on whose behalf it is being conducted (14); be consistent with the actual characteristics, access and usage conditions of the goods and services in question (15); not misrepresent or hide the total cost of a good or a service (16); and exercise care where targeted at children, vulnerable or disadvantaged consumers (18).
- Where consumer endorsements are used in advertising and marketing, these should be truthful and transparent, with any material connections between businesses and online endorsers being clearly and conspicuously disclosed (17).

#### UN Guidelines

Section IV. of the *UN Guidelines* sets out six principles that establish benchmarks for good business practices in the conduct of online and offline commercial activities. Two of these address fair business and advertising practices. Guideline 11 (a) states that businesses should deal fairly and honestly with consumers at all stages of their relationship; while 11 (b) states that businesses should not subject consumers to illegal, unethical, discriminatory or deceptive practices, such as abusive marketing tactics.

Section V. contains guidelines that promote the formulation of national policies. Pertinent to the fair business and advertising principle are:

- guideline 14 (d), which promotes clear, concise and easy-to-understand contract terms that are not unfair
- guideline 27, which states that promotional marketing and sales practices should be guided by the principle of fair treatment of consumers and should meet legal requirements
- guideline 28, which states that member states should encourage all concerned to participate in the free flow of accurate information on all aspects of consumer products
- guideline 30, which states that member states should take measures regarding misleading environmental claims or information in advertising and other marketing activities
- guideline 31, which calls on member states to encourage the formulation and implementation by business of codes of marketing ... that receive adequate publicity.



### 2.1.2 Overview of the issue

The nature of online transactions may deprive consumers of some of the cues and mental shortcuts that enable them to manage risks and develop trust offline. As noted at Section 1.3, e-commerce is often impersonal and generally lacks the opportunity to evaluate items prior to purchase. As a result, the online arena can prove fertile territory for fraudulent and deceptive commercial practices, which can undermine both the welfare of consumers and their trust in e-commerce.

Consumers can be deceived as to the nature of the product or service (or of the advertising itself) and subjected to aggressive and/or misleading marketing techniques. Providers can create confusion with and between the trade names or trademarks of competitors. And as Box 2 highlights, because e-commerce presents low barriers to entry for new providers, including any entity seeking to imitate established brands, fraudulent operators can mimic legitimate websites and manipulate search engine results to drive consumers towards their sites (and scams).

Businesses might also falsely represent themselves as consumers and post reviews that inflate their own reputations and/or denigrate those of competitors (see below). In seeking to gain a competitive advantage over competitors who offer superior goods and services and/or lower prices, providers might also exaggerate the quality or misrepresent the features of their products or services (UNCTAD, 2017a).

#### BOX 2. COPYCAT WEBSITE FRAUD

In March 2018, following an investigation by the United Kingdom's National Trading Standards eCrime team, six people were convicted and sentenced for operating websites that mimicked the official websites of 11 government agencies and departments. Search engine results were also manipulated to make the websites appear more genuine. The fraudsters knowingly misled hundreds of thousands of consumers into paying vastly inflated prices for a number of government services, including new or replacement passports, driving licences and the London Congestion Charge.

The criminals also set up websites that mimicked the official visa sites of other countries (including the United States and Turkey), where travellers could apply and pay for electronic visas to visit those countries. In all cases, the sites offered little or no additional value to consumers using them. It is believed that in addition to consumers in the United Kingdom, Indian, Turkish and US citizens were also defrauded.

Source: NTS (2018), "Six sentenced for large copycat website fraud", <http://bit.ly/2p1gRFR>.

### Misleading pricing

Providers can also present and frame prices in ways that exploit consumers' behavioural biases and (mis)lead them towards sub-optimal choices, e.g. by failing to disclose all elements of the price or underlying conditions (failing to indicate that a certain price is only available if a consumer enters into a two-year contract, for example) and by using misleading reference pricing, or drip pricing strategies.

Reference pricing is the practice of listing a price along with a reference to another (higher) price – e.g. the pre-sale price, a competitor's price, the recommended retail price, or a post-sale price. While traditional economic theory suggests this shouldn't have any impact, behavioural studies show that reference prices influence consumers' assessment of value (Ahmetoglu et al., 2010; OECD, 2018c). A case study on the use of misleading reference prices by a major online retailer in North America is provided in Box 3.

Drip pricing is the practice of advertising a product or service at a certain (lower) price, but incrementally disclosing (“dripping”) additional non-avoidable fees or surcharges as the consumer progresses through the stages of a transaction. This can result in consumers paying a higher price than advertised, or spending more than they realise (ACCC, 2014a). It can trigger consumers’ behavioural biases, including anchoring and endowment effects (Box 14), where consumers feel committed to a purchasing decision and stick with it despite the price increasing during the transaction process. Drip pricing can also increase purchase intentions and price and value satisfaction, and reduce search intentions (Xia and Monroe, 2004; OECD, 2018c). As highlighted in Box 4, consumer protection agencies in Australia, Canada and the United Kingdom have been active in taking enforcement actions against drip pricing (OECD, 2017c).

### BOX 3. MISLEADING REFERENCE PRICES: THE PEOPLE OF THE STATE OF CALIFORNIA V. OVERSTOCK.COM

In 2010, state-level district attorneys in California filed a civil lawsuit against Overstock, a major online retailer in North America, charging violations of California’s Unfair Competition Law (§ 17200 et seq.) (UCL) and the False Advertising Law (§ 17500 et seq.) (FAL). The lawsuit alleged that the company had:

- “routinely and systematically” made untrue and misleading claims about the prices of its products
- displayed average reference prices (ARPs) that were misleading because, among other things, the company directed its employees to select the highest price that they could find as an ARP, or constructed an ARP using a formula that applied an arbitrary multiplier to Overstock’s wholesale cost
- failed to implement any process or procedure to confirm that, for any given list price, there actually existed at least one instance of a sale at the list price stated in the advertisement.

In one example cited in the complaint, Overstock had advertised a patio set for sale for USD 449.99, claiming the “list price” was USD 999. On ordering the patio set, a consumer discovered it still displayed a store price tag of USD 247. The claimed 55% saving against the “list price,” was therefore shown to be misleading.

The Superior Court found the company liable for violating California’s false advertising and unlawful business practice laws. It imposed a fine of USD 6.8 million against Overstock and required the company to more accurately display reference prices and consumer disclosures (Moynihan, 2014). The ruling was upheld on appeal in 2017 (Lally and Goldberg, 2017).

Sources: Moynihan (2014), “California court imposes \$6.8 million in civil penalties against Overstock.com for allegedly deceptive price comparisons”, <http://bit.ly/2Ftpkbr>; Lally and Goldberg (2017), “Upper court underwhelmed by overstock”, <http://bit.ly/2leSANJ>.

In 2015, members of the International Consumer Protection and Enforcement Network (ICPEN) recognised misleading and inadequate information disclosures related to pricing information as a key problem for online consumers. As part of an internationally co-ordinated “sweep” (for a description of Internet sweeps see Section 3.4.1) of online pricing practices in travel and tourism, ICPEN members identified misleading or deceptive conduct such as drip pricing, false reference prices and best price claims, non-existent discounts and time-sensitive representations, and a lack of cancellation and refund information (OECD, 2017a).

### Ratings, reviews and endorsements

Consumers increasingly inform their purchasing decisions by consulting the online reviews and ratings given by their peers. The United Kingdom’s Competition & Markets Authority (CMA) has estimated that GBP 23 billion (USD 28.5 billion) per year of consumer spending in the United Kingdom is influenced by online reviews (CMA, 2015a). The 2017 *Ipsos Global Trends* study<sup>7</sup> found that 70% of consumers agree with the statement: “What I

read about other people's good or bad experiences influences the companies or brands I choose" (Ipsos, 2017). Among the G20 economies, the figure was highest in Indonesia (85%) and lowest in France (57%).

Authentic reviews benefit consumers by providing unbiased information and peer feedback on the quality of products and services. Consumers can use reviews to assess and question information provided by businesses. They can also be empowered to share their own experiences. Reviews and ratings also create a feedback loop for businesses, which can inform the continued improvement of products and services (OECD, 2017a).

The growth of peer platform markets (PPMs), where reviews and ratings systems can help consumers build trust in unknown sellers (and unknown buyers, if acting as a peer provider), has further increased the influence of peer feedback. Businesses are also increasingly using reviews as a form of advertising for their products or services, which underlines the importance of making sure reviews and endorsements in PPMs are not misleading (ICPEN, 2016).

However, the rapid increase in the use of these tools and the influence they can have on consumer decisions has given rise to concerns about their trustworthiness. For example, questions have arisen as to whether reviews are truly representative of consumer experiences (European Commission, 2017a). Specific issues include reviews that are fake, such as those where a provider or its agents pose as consumers and post positive feedback regarding its own services; and reviews used in business advertising, where the promoter fails to disclose material connections to the advertiser. While the latter may be more prevalent than the former, both can mislead consumers into making decisions that they might not otherwise have made, resulting in financial loss and diminished enjoyment of those goods and services. According to different estimates, fake reviews represent between 1% and 16% of all consumer reviews (EPRS, 2015).

Closely related to reviews are product endorsements, testimonials and other statements that draw on the experience an individual has had, or gives the impression of having had, with a product or service. As consumers have gained access to tools that enable them to share their interests, passions and experiences, some have gained a considerable following as bloggers, YouTube "vloggers" or social media "influencers". Brands have looked to leverage the influence and reach of some individuals by providing incentives, such as payments and gifts (including free merchandise), in return for product profile and endorsement. In other instances, people have used social media to actively promote businesses they have a direct commercial stake in, without disclosing their material interest in that business. These practices risk compromising the integrity of an endorsement and can mislead consumers if the commercial relationship is not transparent and/or the endorsement makes misleading claims. Endorsements made by conventional celebrities via social media channels can pose many of the same issues (OECD, 2017a; Fair, 2017a). In the United States, the FTC has carried out extensive enforcement work on this issue. This has included charges against two social media influencers who endorsed an online gambling service while failing to disclose they jointly owned the company; along with warning letters to prominent social media influencers and the issuing of guidance (FTC, 2017a).

### Digital comparison tools

Another aspect of the changing consumer information environment is DCTs (sometimes also called price comparison websites). These have become a popular type of consumer tool in many sectors such as insurance, utilities, real estate rental and buying, car rental and buying and travel. DCTs can increase convenience and reduce search costs by enabling consumers to gather and compare information on price and quality in one place, often in accordance with parameters that can be customised to reflect individual preferences. A consumer survey by the UK CMA found that that 85% of UK consumers with access to the Internet have used a DCT at least once. The CMA estimates that during 2015, UK consumers made 11 million transactions through the largest DCTs in just four sectors (broadband, credit cards, home and motor insurance) (CMA, 2017).

However, the benefits and utility of DCTs can be undermined by misleading and deceptive advertising, and inadequate disclosure. A 2013 study commissioned by the European Commission found that two-thirds of

consumers using comparison tools had experienced a problem in the process, such as the unavailability of the product advertised on the seller's website (32%) or incorrect prices (21%). Most of the comparison tools tested did not disclose information on their business model, including their relationship with suppliers (European Commission, 2013b). The extent to which a comparison tool's operator is transparent as to whether it offers consumers a whole of market comparison, or a restricted one (e.g. listing only providers with which it has a commercial relationship), is a related issue (CMA, 2017).

In 2016, the European Commission and EU consumer protection authorities undertook a co-ordinated sweep of 352 price comparison and travel booking websites across the European Union. The exercise revealed a series of irregularities in online comparison tools, including in relation to misleading prices. Among other things, the findings revealed that:

- In 32% of cases, the price on the page of the comparison list was not the same as the price ultimately displayed in the booking page.
- On 30% of the websites, the total price (inclusive of taxes), or the way this was calculated, was not clear.
- 21% of the websites presented special prices, which were not then available as advertised at the actual booking page.
- 26% of the websites gave the impression that certain offers were scarce (e.g. "only 2 left", "only available today") without specifying that this scarcity applied strictly to their own website (European Commission, 2017g).

### 2.1.3 Examples of good practice

The following section provides examples of steps that have been taken to address a number of the issues outlined in this section.

#### Institutional guidance and self-regulation in online advertising

The Federal Trade Commission of the United States (FTC) has developed numerous recommendations on how to make clear and conspicuous disclosures in digital advertising, including newer forms such as social media and native advertising. The general principle is that advertising must tell the truth and not mislead consumers, all claims must be substantiated, and disclaimers must be clear and conspicuous (FTC, 2013).

UNCTAD has stated that self-regulation of digital advertising has yielded tangible results. There are, it notes, multiple initiatives in developed countries, such as the codes adopted by the European Advertising Standards Alliance<sup>8</sup> and the Interactive Advertising Bureau's Self-Regulatory Principles for Online Behavioural Advertising in the United States.<sup>9</sup> In addition, the Latin American Network of Advertising Self-Regulation Organizations (CONARED)<sup>10</sup> was created in 2007 to promote responsible advertising and freedom of speech (UNCTAD, 2017a).

**BOX 4. ENFORCEMENT ACTIONS ON “DRIP PRICING”****United Kingdom (airline companies)**

In 2011, the United Kingdom’s Office of Fair Trading (OFT)<sup>1</sup> commenced an investigation into airlines that were charging consumers additional debit card payment fees that were not included in the headline price, and were only presented to consumers at the end of the booking process. Credit card charges were also not being presented in a clear and transparent way. The OFT considered these practices to be a breach of provisions on unfair commercial practices, including misleading actions and misleading omissions. In July 2012, the OFT closed the investigation and 12 airlines agreed to include debit card surcharges in the headline price and present any credit card surcharges in a way that could be easily found by consumers (OFT, 2012).

**Australia (accommodation service providers)**

The Australian Competition & Consumer Commission (ACCC) found two accommodation service providers to be in breach of the Australian Consumer Law for making misleading representations by failing to adequately disclose mandatory fees to consumers. One provider did not present a mandatory service fee and cleaning fee on search results pages and accommodation listing pages on its website, mobile site and apps. The other provider failed to adequately present mandatory service fees and payment fees on its mobile site and app, and on particular pages of its website. In October 2015, the ACCC accepted court enforceable undertakings (a type of administrative settlement – see Box 9) by the two providers (ACCC, 2015).

**Australia (ticket sellers)**

The ACCC identified that two ticket selling companies had failed to state a single minimum total price (as required under the Australian Consumer Law). Unavoidable fees, including debit card or credit card fees, a service/delivery fee, and a handling fee, were not properly presented to consumers early in the online booking process. By October 2014, following the ACCC’s investigation, both companies had improved their pricing practices (ACCC, 2014a).

**Canada (car rental companies)**

In February 2018, the Competition Bureau of Canada announced an agreement with a major car rental company to correct misleading advertisements. The Bureau concluded the addition of mandatory fees resulted in services not being available to consumers at the prices advertised, with the additional fees increasing advertised prices by as much as 48%. Prices had been advertised across various media, including online, on mobile applications and in emails. The company will pay a penalty of CAD 1 million and review its practices to ensure that its advertisements comply with the law. This is the third time the Bureau has taken action to resolve similar concerns in the car rental industry in recent years. Its actions have led to a total of CAD 5.25 million in administrative monetary penalties against the three largest car rental companies in Canada (Competition Bureau Canada, 2018).

1. The OFT was abolished in 2014, with many of its functions being assumed by the newly created CMA.

Sources: OFT (2012), “Airlines to scrap debit card surcharges following OFT enforcement action”; ACCC (2015), “Airbnb and eDreams give undertakings to ACCC for improved pricing practices”, <https://www.accc.gov.au/media-release/airbnb-and-edreams-give-undertakings-to-accc-for-improved-pricing-practices>; ACCC (2014a), “ACCC investigation leads to clearer ticket pricing” <http://bit.ly/1tauM9e>; Competition Bureau Canada (2018), “Enterprise Rent-A-Car Canada to pay a \$1 million penalty for advertising unattainable prices”; and adapted from OECD (2017c), “Use of behavioural insights in consumer policy”, <http://dx.doi.org/10.1787/c2203c35-en>.

## Innovation to improve the integrity of reputation systems

Enhanced system design can support more honest feedback and mitigate risks relating to fraudulent and dishonest consumer-to-business (C2B) feedback in unilateral reputation systems (e.g. third-party platforms offering and facilitating reviews of restaurants and hotels etc.). For example, the evolution of these systems has seen the emergence of a new generation of review platforms that seek to address concerns around integrity by seeking and accepting reviews only from verified purchasers. Technology will also have a role to play in this respect, e.g. by using algorithms to identify and alert platform providers to rogue reviews (Soper and Cao, 2015). Better design can also counter instances of retaliatory feedback or tacit collusion in bilateral P2P reputation systems. For example, Airbnb introduced a “double blind” review system in 2014, where hosts and their guests only see reviews received from the counterparty after both parties have completed their assessment of each other, or after the deadline for providing reviews has expired (Airbnb, 2014). A recent OECD survey on peer platforms found that 56% of peer consumers agree that other peer platforms should adopt this policy (OECD, 2017d).

## 2.2 Appropriate disclosures

### Statement of the principle

E-commerce businesses should provide clear and accurate disclosures about themselves, the goods or services offered, and the transaction conditions, so that consumers have sufficient information to make an informed decision about a transaction.

### 2.2.1 Summary of the international instruments

#### OECD Recommendation

Part C of the *Recommendation* provides general principles that outline the form and timing of disclosures (provisions 25-27), followed by specific details concerning the content of disclosures. The general principles specify that online disclosures should be:

- clear, accurate, easily accessible, conspicuous and made at the relevant time in easy-to-understand language
- available in the same languages as those used for the undertaking of transactions, with all references to costs provided in the applicable currency
- provided in a way that enables consumers to retain a complete, accurate and durable record
- cognisant of the device or platform over which the transaction occurs (i.e. recognising the growth in the use of mobile devices with smaller screens).

Provisions addressing the content of online disclosures specify that businesses should provide information concerning:

- themselves (28-30), including location, contact details, dispute resolution procedures, and membership of self-regulatory programmes, business associations, and dispute resolution bodies (including how to contact them)
- the goods or services offered (31-32), including functionality and interoperability, technical or contractual conditions that might affect a consumer’s ability to access or use the good or service (i.e. recognising issues that can arise in relation to digital content), safety information, and any age restrictions
- the transaction’s terms and conditions (33-35), including in relation to prices, charges and costs (including renewals and recurring charges and ways to opt out from these), methods of payment, contract duration, terms of delivery, conditions related to contract withdrawal, cancellation, after-sales and returns, exchanges,

refunds, warranties and guarantees, the privacy policy, and information on available dispute resolution and redress options.

The overarching goal is that consumers should have sufficient information to know the price and attributes of the product or service under consideration, as well as the terms and conditions of sale, of payment and delivery, and their after-purchase rights (OECD, 2018c).

### UN Guidelines

Guideline 5 (e) recognises “access by consumers to adequate information to enable them to make informed choices according to individual wishes and needs” as a legitimate need. Guideline 11 (c) promotes good business practices on disclosure and transparency. It states that businesses should provide complete, accurate and not misleading information regarding the goods or services, terms and conditions and final costs, and should ensure easy access to this information regardless of the technology used.

Guideline 14 (b) promotes national policies that encourage clear and timely information – including the identity of the business, its legal name, principal geographic address, website, e-mail address and telephone number – that enables consumers to contact businesses easily; and enables regulatory and law enforcement authorities to identify and locate them. Guideline 14 (c) refers to clear and timely information regarding the goods or services offered, and the terms and conditions of the relevant transaction.

### 2.2.2 Overview of the issue

In order to make informed purchasing decisions when undertaking e-commerce transactions, consumers need relevant and accurate information concerning goods and services and the vendors who are supplying them (UNCTAD, 2017a). Effective, well-targeted information can assist consumer decision making and facilitate product comparisons. It can also increase transparency and accountability, reduce search costs, help to prevent disputes and protect consumers from deceptive practices (OECD, 2010a). Given e-commerce is, for the most part, remote and impersonal, disclosures are relied upon to play a key role in communicating information to consumers.

Online disclosures can encompass information about the business, the goods and services on offer, and the transaction itself, including information about payment methods, privacy policies and available dispute resolution and redress options. Businesses may make such disclosures through advertising and marketing, contractual terms and conditions, and legally required notices. This information can be conveyed in different ways, including through pop-ups, links, text, images, audio and video. The provision of information takes place at different points throughout the transaction journey, including pre-transaction advertising and marketing; and information displayed during the course of the transaction, including during the payment process (OECD, 2018c).

### Information asymmetries in e-commerce

Information asymmetries occur whenever sellers know more about the features and quality of their products than buyers do. While effective competition may encourage businesses to provide some information to consumers, the absence of broader disclosure requirements might lead to businesses only disclosing information that improves their chances of making a sale (OECD, 2018c). The remote nature of the Internet and the complexity and non-negotiability of terms and conditions – including privacy notices (see Section 2.4) and end user licence agreements (see section on digital content, below) – can exacerbate information asymmetries, especially when it comes to “experience” goods (whose attributes or qualities can only be observed after use) and “credence” goods (whose attributes or qualities cannot readily be determined by the purchaser even after purchase and use).<sup>11</sup>



## Effective disclosure is a challenge

Information that is not well designed can be useless or even counterproductive for consumers (OECD, 2010a). Behavioural research has shown that the ways in which information is presented or framed can have a dramatic effect on how consumers respond to that information. For disclosures to be effective, they must be carefully designed. Key challenges in this respect relate to the volume and complexity of information that consumers can face. As Box 5 highlights, research frequently shows that consumers rarely read the privacy notices, or the terms and conditions presented to them and that presenting effective information disclosures is challenging (OECD, 2017b).

### BOX 5. DO CONSUMERS READ ONLINE TERMS AND CONDITIONS?

The nature of online terms and conditions, including privacy policies and end user license agreements (EULAs), rarely encourage consumer engagement. They are frequently inordinate in length, impenetrable in their language and inflexible in their application (i.e. the consumer is faced with a “take it or leave it” choice).

Research undertaken for the European Commission found that while between 90% and 95% of consumers accept online terms and conditions, very few read these in full. Readership varied depending on how the terms and conditions were presented. Where consumers had to click through to terms and conditions, only 9.4% opened them, whereas 77.9% of consumers said that they at least scanned terms and conditions that could be scrolled through (Elshout et al., 2016).

The 2017 *Ipsos Global Trends* survey found that, across the 23 countries featured, 64% of respondents agreed with the statement that “I often don’t bother fully reading terms and conditions on a website before accepting them” (Ipsos, 2017). Among G20 economies, that figure was highest in Great Britain (73%) and lowest in Brazil (52%). However, self-reporting by consumers may be prone to overstating the actual figure. Server-side surveys indicate that barely 1% of consumers actually read terms and conditions (Ipsos, 2014).

Readership of EULAs appears to be even lower, with only 0.2% of consumers accessing EULAs (Bakos, Marotta-Wurgler and Trossen, 2014), a situation that the requirement of obtaining consumer consent does little to improve (Marotta-Wurgler, 2012). It has been calculated that the median time spent on software EULAs is six seconds, with at least 70% of users spending less than 12 seconds on the license page (Sauro, 2011). A documentary film concerning online terms and conditions asserts it would take an average of one month per year for consumers to read the terms they are presented with (Terms & Conditions May Apply, 2013).

*Sources:* Elshout, et al. (2016), “Study on consumers’ attitudes towards terms and conditions (T&Cs): Final report”, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2847546](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847546); Ipsos (2017), “Ipsos Global Trends: 8. Online behaviour”, <https://bit.ly/2HJnUK>; Ipsos (2014), “Global trends 2014: Navigating the new”, <http://bit.ly/2FEMmiA>; Bakos, Marotta-Wurgler and Trossen (2014), “Does anyone read the fine print? Consumer attention to standard-form contracts”, <https://doi.org/10.1086/674424>; Marotta-Wurgler, (2012), “Does contract disclosure matter?”, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2736521](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736521); Sauro, (2011), “Do users read license agreements?”, <https://measuringu.com/eula>; Terms & Conditions May Apply (2013).

In addition, the channel through which the information is presented to the consumer can have an impact on its utility. What works for a recipient of a print disclosure may not work when transferred to another recipient’s “screen of choice”, be it a computer monitor, tablet or a mobile device (Benartzi and Lehrer, 2017). Different delivery channels for consumer disclosures may require businesses to optimise both the format and content of information (OECD, 2018c).



### The downsides of unread disclosures

Surveys have attempted to quantify the extent of consumer detriment that can arise from the non-reading of online terms and conditions. In a 2011 survey of British consumers, 21% reported that they had suffered from agreeing to terms and conditions they did not fully read: 10% were locked into longer contracts than expected and 5% were unable to cancel or amend a hotel or holiday booking (Smithers, 2011). Similarly, research undertaken for the European Commission surveyed consumers in the Netherlands and Poland to determine the extent of consumer harm that arises from not reading or not fully understanding terms and conditions. It found that 26% of respondents had encountered a problem in the 12 months prior to the survey, two-thirds of which were associated with online purchases. Delivery issues were the main problem, followed by issues relating to returns.<sup>12</sup> While the costs associated with these problems were generally low (below EUR 100 for more than three in five respondents), over half of those who experienced a problem considered it to be serious (Elshout et al., 2016).

Box 6 highlights a range of the consumer detriments that are associated with online terms and conditions.

#### BOX 6. CONSUMER DETRIMENT ASSOCIATED WITH ONLINE TERMS AND CONDITIONS

**High search costs:** search costs, namely time, are likely to be high if online terms and conditions lack transparency or are long and complex. This can increase costs for consumers when comparing offers, or in determining what they agreed to when something goes wrong.

**Hidden fees and costs:** if online terms and conditions are not clear, or are agreed to without reading, consumer detriment may occur if there are hidden fees, costs or charges in the terms and conditions.

**Selecting the wrong product/service:** if consumers do not read or understand terms and conditions they may fail to select the product or service that best suits their needs. This has costs for the consumer and, to the extent that this is widespread behaviour, for the broader market.

**Low quality products or services:** opaque terms and conditions (or accepting without reading) could lead consumers to make purchases that are of a lower quality than anticipated. This could be because elements of the quality of a product or service are buried in the terms and conditions and not fully factored into the consumer's decision making.

**Lock-in:** lock-in occurs where consumers are required to stay with a particular business, product or service despite wanting to change. Terms and conditions could lock consumers in directly through automatic contract renewal, or where high switching costs and/or the prospect of leaving behind personal data and/or networks act as a barrier to consumer switching, for example.

**Disclosure of personal data:** if consumers do not read or understand privacy notices they may unwittingly share personal information or agree to provide such information to third-parties, or agree to their data being used in ways they would not knowingly approve of.

Source: Reproduced from OECD (2018c), "Improving online disclosures with behavioural insights", <https://bit.ly/2KFolHN>

### Disclosure and digital content

Disclosure can and should play a particularly important role in relation to consumers' purchases of, or subscriptions to, intangible digital content – not least by enabling consumers to comprehend limitations they might face in the use of digital products they have purchased or subscribed to.

Markets for intangible digital content products have seen rapid growth. For example, in the music industry – the sector that was first to feel the full force of Internet-fuelled disruption – streaming became the largest source of global recorded music sales in 2017, with revenues from services such as Spotify and Apple Music rising by 37% and surpassing sales of physical formats for the first time (Bond, 2017). Other channels through which digital content can be purchased or subscribed to include e-commerce platforms, video streaming platforms, the platforms of software houses, video game environments, “app” stores, Internet Protocol (IP) TV, and social media platforms.

Limitations on consumers’ abilities to utilise digital content they have purchased can stem from copyright law, as well as the terms and conditions that providers assert in EULAs and other terms of service. Such limitations can vary, sometimes significantly, from one product to another, with restrictions on similar products varying between different service providers. For example, the period over which a consumer may be able to use a product may be limited, or indefinite; copying beyond private use may or may not be permitted; or the number of times a product (such as a piece of music or an e-book) can be accessed, streamed or downloaded may be limited (functionality limitations) (OECD, 2014a).

Moreover, consumers may not always be able to access a product that they have lawfully acquired in one jurisdiction while travelling in another; and they may be unable to acquire a digital content product offered by businesses located in other jurisdictions (geographical limitations). Further, consumers may be unable to play, listen to, or watch a product on different devices (interoperability limitations) (OECD, 2014a). There may also be conditions or limitations on sharing a product with, or selling a product to, other parties.

Some surveys reveal that consumers are often unaware of these limitations, which can cause significant detriment in some cases. Findings of this nature are perhaps unsurprising, given that some digital content providers do not disclose material information to consumers in a clear, conspicuous and unavoidable manner; including any limitations on functionality, usage while abroad, or interoperability. And, as highlighted in Box 5, the terms and conditions included in EULAs and terms of service provisions are, in many instances, long, complex and not easily accessible (OECD, 2014a).

### 2.2.3 Examples of good practice

#### Mandated online disclosure requirements by country

A number of G20 economies have mandated online disclosure requirements, with varying degrees of specificity. The following provides an overview of a selection of these and is based on a report from the OECD concerning the use of behavioural insights to improve online disclosures (OECD, 2018c).

**Canada:** eight Provinces have adopted the Internet Sales Contract Harmonization Template<sup>13</sup> which lists 13 pieces of information that online businesses must provide to consumers. These requirements were developed to be consistent with the OECD’s 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD, 1999a) (which are largely consistent with the updated e-commerce *Recommendation*).

**Mexico:** in Mexico the requirements are more high-level, requiring businesses to provide only their address and telephone number. However, Mexican law also provides consumers with the right to know all the information about the terms, conditions, costs, additional charges (if any), and payment forms for the goods and services offered by businesses.

**United States:** there are no specific types of information that businesses are required to provide to consumers under federal law. Instead, the Federal Trade Commission Act prohibits businesses from engaging in unfair or deceptive acts. The practical implications for what businesses should disclose online have been developed through case law and FTC guidance<sup>14</sup> – including rules, enforcement policy statements, formal guidelines, and

informal staff guidance. In addition, there are a number of state-based laws and rules that require particular businesses to provide certain types of information to consumers. For example, the California Civil Code § 1789.3 requires e-commerce providers to inform consumers of the name, address, and telephone number of the provider, consumer charges, and dispute resolution.

**European Union:** online businesses are required to satisfy 20 items under Article 6 of the Consumer Rights Directive. These include details about the good/service, the trader, price information, consumer rights and guarantees, payment and delivery details, contract details, interoperability of digital content, and consumer redress.

In other jurisdictions businesses are encouraged (rather than required) to provide similar types of information. For example, the Government of Australia's *Guidelines for Electronic Commerce* recommend that online businesses provide various types of information to consumers, largely consistent with the information listed in the *OECD Recommendation* (Government of Australia, 2006).

### OECD Consumer Policy Guidance on Intangible Digital Content Products

The *OECD Consumer Policy Guidance on Intangible Digital Content Products* (OECD, 2014a) (hereafter *Guidance*) provides a set of policy principles for addressing a range of the challenges that consumers can encounter when acquiring and using intangible digital content products, including inadequate information disclosure. Designed to complement the 1999 e-commerce guidelines, the *Guidance* covers issues concerning: i) digital content product access and usage conditions; ii) privacy and security; iii) fraudulent, misleading and unfair commercial practices; iv) children; v) dispute resolution and redress; and vi) digital competence. Common to all these areas is the requirement for effective information disclosures.

## 2.3 Effective processes for transaction confirmation and payment

### Statement of the principle

E-commerce businesses should not process a transaction unless the consumer has given express consent, and should provide easy-to-use payment mechanisms with appropriate limitations on consumer liability for unauthorised uses.

#### 2.3.1 Summary of the international instruments

##### OECD Recommendation

Part D of the *Recommendation* addresses transaction confirmations, while Part E addresses payments. Part D specifies that businesses should:

- ensure the point at which consumers are asked to confirm a transaction, after which payment is due or they are contractually bound, is clear and unambiguous, as should be the steps needed to complete the transaction, especially for new payment mechanisms (36)
- provide opportunities for consumers to review summary information about the good or service and delivery and pricing prior to confirming a transaction; and to identify and correct errors or modify or stop the transaction (37)
- refrain from processing a transaction unless the consumer has provided express, informed consent to it (38)
- provide a device-appropriate record of the transaction for the consumer to retain (39).

With regards to payments, Part E specifies that businesses should offer easy-to-use payment methods, the security of which should be commensurate with payment-related risks (40).

Further, it calls on governments and stakeholders to work together to:

- develop minimum levels of consumer protection across payment mechanisms, including regulatory or industry-led limitations on consumer liability for unauthorised or fraudulent charges; and develop payment arrangements that may enhance consumer confidence in e-commerce, such as chargeback mechanisms and escrow services (41)
- explore greater harmonisation of payment protection rules among jurisdictions and seek to clarify how issues involving cross-border transactions could be addressed when payment protection levels differ (42).

### UN Guidelines

At Section V, Part A, guideline 14 (e) promotes national policies that encourage “a transparent process for the confirmation, cancellation, return and refund of transactions”. Guideline 14 (f) promotes national policies to ensure “secure payment mechanisms” (UNCTAD, 2017a).

At Section V, Part J, which is dedicated to financial services, guideline 66 (g) calls on member states to establish or encourage “appropriate controls to protect consumer financial data, including from fraud or abuse”.

### 2.3.2 Overview of the issue

#### Payment methods

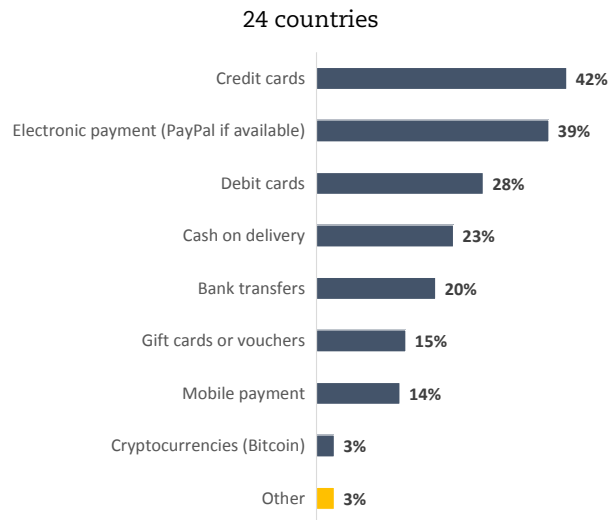
Depending on the provider and the jurisdiction in which the purchase is being made, consumers typically have a number of options available to them for making online payments. These range from more traditional payment methods, such as debit cards, credit cards, bank transfers and even cash on delivery, to payment services that are native to the Internet, including electronic payment intermediaries (e-wallets, including electronic escrow systems), mobile payments and, in some cases, cryptocurrencies. Accepting payment methods that consumers have access to and can easily use is key to increasing engagement in e-commerce; and ensuring those payment systems are secure is a fundamental building block of consumer trust.

Figure 3, from the CIGI’s 2017 *Global Survey on Internet Security and Trust* (CIGI, 2017), highlights findings on consumers’ preferred means of online payment. It should be noted that the global figure masks wide variations between the 16 G20 economies covered by the survey. To some extent these will reflect the characteristics of respective countries, including whether banking systems are widely used and the conditions under which e-commerce has developed. For example, CIGI found that credit cards are preferred by 72% of South Korean consumers, compared to 15% of French consumers. E-wallet payments such as PayPal are preferred by 69% of Italian consumers, but by only 5% of their Japanese counterparts. Mobile payments are preferred by 44% in China, compared to just 2% in Great Britain (CIGI, 2017).

In developed regions, online payments are dominated by credit and debit cards, followed by e-wallets. In developing countries, by contrast, credit cards are rarely the most important payment method for e-commerce, and the uptake of digital payments is often low. In China, the home-grown Alipay and WeChat Pay mobile financial apps are often considered to be the main drivers of domestic e-commerce growth. Alipay, an escrow-based system, is used by 68% of all online shoppers in China (UNCTAD, 2017a; UNCTAD, 2017b).

For cross-border purchases, e-wallets appear to be particularly popular as a method of payment. A 2017 survey of cross-border e-commerce shoppers across 31 countries found that e-wallets (such as PayPal and Alipay) were the preferred choice for 39% of the respondents, followed by credit cards (28%) and debit card/bank transfer (20%) (IPC, 2018). However, it is worth noting that a lack of interoperability in payments systems can serve as a major obstacle to cross-border transactions (UNCTAD, 2017a).

**Figure 3.** Preferred means of paying for goods and services online globally



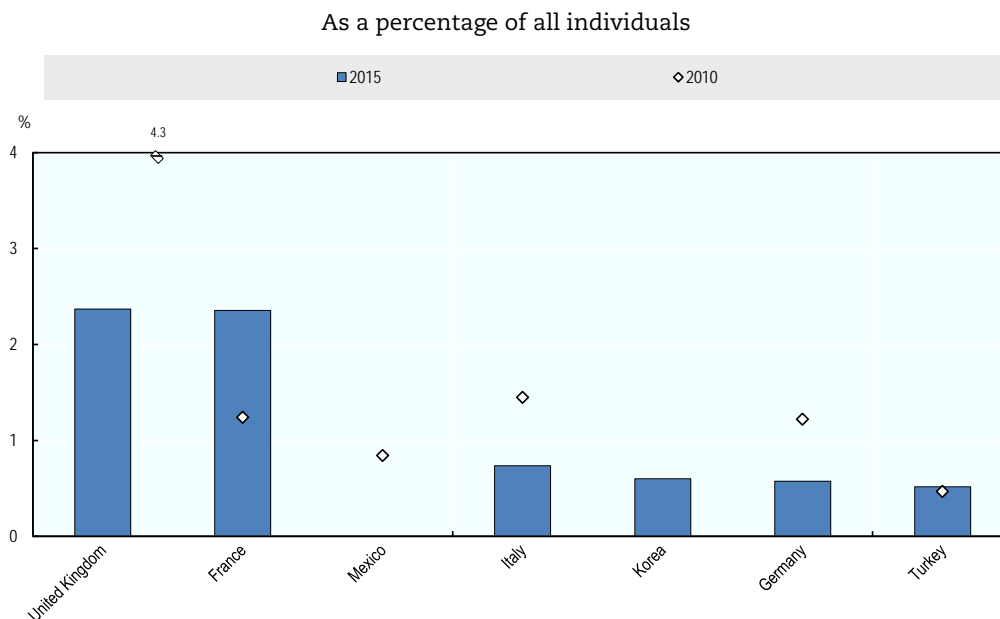
Note: Base = buy goods or services online at least once a month (n = 18 551).

Source: CIGI (2017), 2017 CIGI-Ipsos Global Survey on Internet Security and Trust, [www.cigionline.org/internet-survey](http://www.cigionline.org/internet-survey).

### Online payment security

Without adequate payment security, consumer data provided in the context of e-commerce payments could be lost, stolen or otherwise misused. The situation is of particular concern in the case of payments made using mobile devices, due to the higher risk of the devices being lost, stolen or otherwise compromised. Although the advance of technology offers the potential for increased data security, consumer concerns about the level of protection remain, and may impede the use of mobile payments systems. Mobile devices that employ end-to-end encryption and dynamic data authentication, if utilised, could help to address concerns, thereby increasing consumer confidence in mobile payments (OECD, 2014b).

**Figure 4.** Individuals having experienced a financial loss from fraudulent online payments in the last three months



Note: Data for Mexico refer to 2009 instead of 2010.

Sources: OECD (2017a), *OECD Digital Economy Outlook 2017*, <http://dx.doi.org/10.1787/9789264276284-en>; OECD (2018d), *ICT Access and Usage by Households and Individuals* (database), <http://oe.cd/hhind>.

The findings from a 2016 survey, which focused on six G20 economies, show a majority of consumers surveyed across Argentina (73%), France (68%), Germany (56%), China (71%), South Africa (71%) and the United States (69%) either “somewhat” (35-42%) or “strongly” (18-38%) agreed with the statement: “I am concerned that the payment information I provide online may be stolen and misused” (Institute for Consumer Policy, 2017). As Figure 4 highlights, OECD data show that these concerns reflect the actual detriment that some consumers have experienced.

### Disparities in protections offered by payment mechanisms

Consumers can benefit considerably by using payment mechanisms that provide high levels of protection, even if they have to pay a premium for that coverage. Such protection helps consumers to avoid the detriment that would otherwise arise when they are the victims of fraud or unauthorised payments. In these instances, payment providers may offer the only effective means for obtaining redress. This can be particularly important in the case of cross-border transactions, where consumers may have limited means to pursue redress (OECD, 2014b).

However, levels of protection across payment mechanisms can vary from country to country, depending on the payment method used. In most countries, consumers making a payment with a credit card benefit from the protections attached to such cards, typically in the form of a chargeback mechanism. Chargeback is a legal right for consumers in the United States and is applied as a contractual right in the European Union (UNCTAD, 2017a). In general, protection for credit cards is higher than for debit cards or bank debits. In the case of the latter, consumers usually face variable liability limits for unauthorised charges, but lack protection in the event of conformity and delivery problems (OECD, 2014b). As noted above, electronic escrow payment methods are popular in China, where they are widely accepted by consumers as a guarantee for their transactions. Even though protections offered by electronic escrow lack a legislative foundation, they are considered to function better than statutory routes to consumer redress in China (UNCTAD, 2017a). Redress is often unavailable when consumers use pre-paid cards, or where charges are collected through their mobile phone bill.

As the above highlights, minimum levels of consumer protection for mobile and online payments are needed, regardless of the payment mechanism used. As noted in Section 2.3.1, this need is addressed by the *OECD Recommendation* (see provision 41), which calls on governments and stakeholders to work towards this goal (OECD, 2017b).

### Effective transaction confirmations

In some instances, consumers engaged in online purchases may not realise they are confirming a transaction. For example, consumers using mobile devices to make “on the go” app purchases might not be aware that, simply by clicking on an icon (e.g. where one-click buying is a feature offered by the vendor), they have agreed to a purchase and that payment is due. As a result, consumers could end up being billed for products they did not intend to buy. On the other hand, consumers may inadvertently supply incorrect payment information and, without their knowledge, have their transaction cancelled or rejected and remain unaware that this has happened. There may also be uncertainty about the status of the transaction when, for example, the connection on a mobile device is lost during the confirmation process (OECD, 2014b). These scenarios highlight the need for effective transaction confirmations.

### Risks to children if effective transaction confirmations are lacking

Children are increasingly using digital content products, such as apps and online games, for entertainment, or to support education and learning. At the same time, the use of mobile devices to make e-commerce purchases in a frictionless manner is also growing (e.g. one-click buying and other features that do not require consumers to re-enter payment information for each purchase). In combination, these two trends have exposed children to a number of risks. Although in most countries children generally do not have the legal capacity to make payment commitments, they have, in many instances, been able to acquire additional product

features or content without their parents' or guardians' knowledge or consent. For example, once children are using an app or an online game, they may be able to incur multiple charges for additional content without always having to enter a password or financial information. The fact that some products may be advertised as "free" or without disclosure of possible additional charges could further complicate the situation, as the account holder (typically a parent or guardian) may not be aware that they or their children could incur charges for acquiring additional digital content products or features while using those products (OECD, 2014a; OECD, 2014b).

Numerous news reports have highlighted this issue, with, in some instances, parents receiving bills amounting to thousands of US dollars (or the equivalent in local currencies) for in-app and in-game purchases made by children without their parents' knowledge or authorisation (Orlando, 2014). Based on a 2013 survey of 2 000 British parents who owned a smartphone or tablet, Microsoft estimated a "monthly spend on unauthorised apps and in-app purchases" of around GBP 30 million across Britain (Trenholm, 2013).<sup>15</sup>

### 2.3.3 Examples of good practice

#### Transaction confirmation processes

In the United States, the FTC's efforts to tackle the issue of unauthorised in-app purchases by children have included the filing of enforcement actions against Apple, Google and Amazon on this issue.

The FTC's settlement with Apple required the company to change its billing practices to ensure it obtains express, informed consent from consumers before charging them for in-app purchases. The company was also required to provide full refunds totalling a minimum of USD 32.5 million to consumers who were billed for accidental or unauthorised in-app purchases that were incurred by children (FTC, 2014a).

Similarly, a settlement reached with Google required it to provide USD 19 million in full refunds for unauthorised in-app charges incurred by children; and to modify its billing practices to obtain express, informed consent from consumers before billing them for in-app charges. Where the company obtains consumers' consent for future charges, consumers must have the option to withdraw that consent at any time (FTC, 2014b).

The FTC's settlement with Amazon could result in refunds of more than USD 70 million for in-app charges to consumers who were affected by Amazon's practices and received charges they didn't expect or authorise (FTC, 2017b).

#### OECD Consumer Policy Guidance on Mobile and Online Payments

The *Consumer Policy Guidance on Mobile and Online Payments* (OECD, 2014b) complements Parts D and E of the e-commerce *Recommendation* and offers a blueprint for helping shape consumer protection and industry practices in the area of mobile and online payments. It seeks to do so in a manner that will remain relevant as the technology used by payment systems continues to evolve. It incorporates the five distinct areas set out below and, as such, offers a response to the range of issues highlighted above:

- 1. information on the terms, conditions and costs of transactions**, including guidance on ensuring:
  - payment-related information is easily accessible, and readable
  - consumers understand payment terms and conditions
  - billing statements are transparent
- 2. privacy and security**, including guidance on ensuring that the collection and use of payment data does not happen in ways that are contrary to consumer interests; and that the security of these data is protected
- 3. confirmation processes**, and ensuring consumers understand when a transaction has been concluded and that payment is due, or that a transaction has not been fully processed



4. **enabling parents or guardians** to monitor and limit children’s mobile and online payments for goods and services
5. **addressing varying levels of protection among payment providers and payment mechanisms**, including guidance on ensuring:
  - consumers are adequately informed about their rights and obligations in payment transactions
  - levels of payment protection ensure consumers are provided with adequate remedies in case of problems.

## 2.4 Measures to address privacy and security risks

### Statement of the principle

E-commerce business practices regarding consumer data should be lawful, transparent and fair, enable consumer participation and choice, and include reasonable security safeguards.

#### 2.4.1 Summary of the international instruments

##### OECD Recommendation

The *Recommendation* notes that consumer data is at the core of many e-commerce services, thus elevating privacy and security risks. It recalls the need to address these risks consistent with other OECD instruments (see below) and, at Part G, features two provisions that are focused on privacy and security, including the dimensions of digital security that may not relate to data. These specify that businesses should:

- protect consumer privacy by ensuring that practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards (48)
- manage digital security risk and implement security measures for reducing or mitigating adverse effects relating to consumer participation in e-commerce (49).

##### Other OECD instruments

The *OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (OECD, 2015b) and *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013), are both relevant to this principle. They provide a set of internationally agreed high-level principles that can be used to drive the development of standards that support security, privacy and trust.

##### UN Guidelines

The revised *UN Guidelines* incorporate matters of privacy for the first time. The General Assembly Resolution (70/186) adopting the *UN Guidelines* recognises that: “Member States have a common interest in promoting and protecting consumer privacy and the global free flow of information” (United Nations, 2015). The actual *UN Guidelines* establish a new legitimate need around “the protection of consumer privacy and the global free flow of information” (Guideline 5 [k]).

Section IV concerns principles for good business practice and contains guideline 11 (e), which encourages businesses to protect consumers’ privacy through: “a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data”. Guideline 14 (h) promotes national policies to ensure consumer privacy and data security.

As noted at Section 2.3.1, guideline 66 (g) calls on member states to establish or encourage “appropriate controls to protect consumer financial data, including from fraud or abuse”.



### 2.4.2 Overview of the issue

Data powers the digital economy and, in the B2C arena, personal data has emerged as a new asset class (Koske, I. et al., 2014c). In e-commerce, data can be as critical to facilitating an online transaction as making a payment. In some instances, personal data is provided in lieu of payment (e.g. for nominally free-to-use services such as social media platforms). The volume of personal data that is collected, processed and stored by business is already vast and will increase further as more people mediate more of their affairs – economic, social and personal – through the Internet and the increasing number of their “things” it connects (e.g. smart home appliances, connected vehicles etc.).

Information such as delivery and billing addresses and payment details are routinely volunteered by consumers when making online transactions. However, the extent to which other types of data – including sensitive personal data – are gathered by a vendor or platform, often remains unclear to consumers, as do the means by which these data are gathered. For example, search habits, purchase history, location and IP address are collected in ways that can be difficult for consumers to understand or prevent.

As Box 7 highlights, online businesses utilise three broad approaches for collecting consumer data. Once collected, they derive value from it by creating new forms of interactions and personalised services; targeting advertising or geo-localised services to help match supply and demand; trading and sharing personal data with third parties to merge disparate data sets together; and by generating new insights about individuals through profiling and by exploiting advanced predictive analytical tools with large data sets (Acquisiti, 2010; OECD, 2015).

Many different entities can have access to the personal data that consumers generate while engaging in e-commerce. In addition to the provider and/or intermediary marketplace, payment providers, search engines, operating system platform providers, hardware manufacturers, mobile operators, content and application developers, data analytics companies, advertisers and coupon and loyalty program administrators may all have sight of elements of these data (OECD, 2014a).

The next generation of e-commerce looks set to become even more data intensive as consumers gain the option of automating routine purchases and delegating decision making in complex markets (e.g. utilities, financial services) to device software and intermediary services that will operate autonomously. The algorithms powering these autonomous services will rely on information from consumers’ smart devices (e.g. to make grocery orders based on tracking a refrigerator’s contents); and data feeds from their service providers concerning consumption histories and spending patterns (e.g. transaction histories from bank accounts and credit cards).

#### BOX 7. THE THREE METHODS OF COLLECTING CONSUMER DATA

Consumer data can be **volunteered** when they are explicitly shared by a consumer (the data subject). Examples include creating a social network profile and entering credit card information for online purchases.

Data can be **observed** when captured by recording activities. In contrast to volunteered data where the data subject is actively and purposefully sharing their data, the role of the observed data subject is passive. Examples of observed data include location data from mobile phones, and web usage behaviour.

And finally, information can be **inferred** as the result of data analytics. Examples include credit score calculations based on an individual’s financial history. Personal information can be “inferred” from several pieces of seemingly “anonymous” or “non-personal” data.

Source: OECD (2015a), *Data-Driven Innovation: Big Data for Growth and Well-Being*, <http://dx.doi.org/10.1787/9789264229358-en>.

### Concerns over data collection practices

Companies' uses of personal data can be beneficial for consumers. For example, data generated by consumer activity online has enabled the provision of "free" services in exchange for these data, a development reflected in the addition of "non-monetary transactions" to the scope of the OECD *Recommendation*. These data are also used to tailor services to consumers' preferences and can also help to improve authentication in order to reduce fraud. The observation of individual behaviour can also serve as a feedback mechanism that enables companies to optimise their products and services for the user (OECD, 2017a). In many instances, observed data is necessary for the product to run or to be updated, or for a service to be delivered. For example, an app provider may access geo-location data and/or IP addresses in order to provide location-based services on mobile devices (OECD, 2014a).

However, the extensive gathering of consumer data can also give rise to a range of concerns. The success and scale of a digital platform is frequently a reflection of the volume of data it gathers about its users and then leverages in its relationship with them. And while a platform's data collection and processing practices can render the consumer transparent to the platform, it is not clear that there is a parallel advance in the transparency of the platform's data practices to the consumer (OECD, 2015a). In addition to data practices being opaque to the consumer, they typically cannot be turned off or opted out of. Given that consumer engagement with online privacy notices and wider terms of use is limited (see Section 2.2), conventional notice and consent mechanisms are unlikely to prove effective in rebalancing this level of information asymmetry.

A platform can utilise algorithms fed by consumer data to shape how consumers experience its services, including its marketing to them, the goods and services they are offered, and the wider content they get to see. The same capabilities could also give platforms the means to personalise prices (Mohammed, 2017), although the extent to which this is happening remains unclear. Inference techniques enable businesses to glean sensitive information from data which may at first appear trivial, such as past individual purchasing behaviour or social media "likes", but which reveal patterns and insights when combined and correlated with other datasets. In one often cited example, the American retailer Target "figured out a teen girl was pregnant before her father did" (Hill, 2012) based on specific signals in historical buying data. In addition, concerns have been raised that the information inferred through data analytics may facilitate aggressive or predatory marketing practices, whereby a company exploits the vulnerabilities of consumers in a way that induces them to purchase goods or services that they would not otherwise have bought (OECD, 2015a).

As a growing number of entities gather increasing amounts of personal data and utilise big data analytics to mine these data, the risk of privacy violations also increases (OECD, 2017a). In addition to challenging the privacy norms that privacy and data protection principles seek to promote (such as data minimisation), these practices can have other adverse consequences. For example, there is the possibility of consumers being discriminated against in credit, insurance, or healthcare markets, based on inferences drawn from data that businesses have collected about them (FTC, 2016a).

Although many countries provide legislative or constitutional protection for privacy and other consumer rights, the effective implementation of those rights is challenging in an era of data abundance, where data flows and business interactions are characterised by a high level of complexity (OECD, 2017a).

### The importance of data security

The growing scale and complexity of online platforms' data infrastructure reflects the need to store and process massive volumes of consumers' personal data gathered via the approaches outlined in Box 7. If a platform has taken insufficient steps to secure its infrastructure, the risks of a data security breach – resulting from either negligence or malicious intent – also grow.

The potential harm to individuals from the misuse of their personal data, whether accidentally exposed or lost, or purposefully stolen, may be significant. Consumers' privacy could be compromised, and significant distress and detriment could result. The impact for an organisation experiencing a data breach can also be severe. They

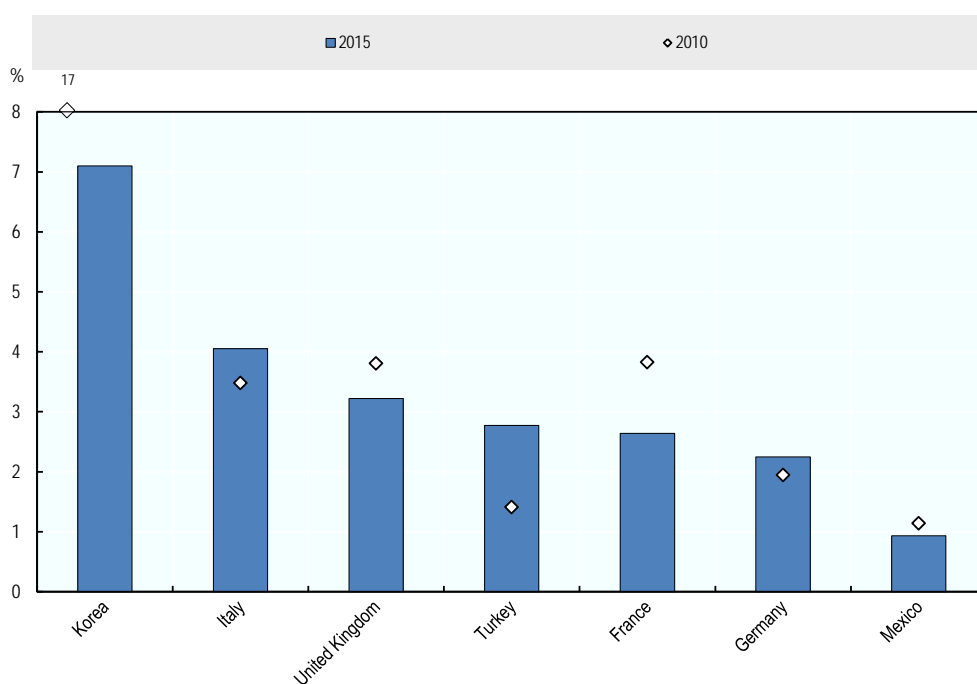
often incur major costs in responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also prove costly, given that a loss of consumer trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals (OECD, 2013).

### The scale of data security incidents

Data breach incidents affecting the confidentiality of personal data have increased in number and severity. For example, in 2005, ChoicePoint (an aggregator of consumer data) was the target of one of the first high-profile data breaches, involving over 150 000 personal records (OECD, 2017a). Contrast that with the 2017 data breach at Equifax (one of the largest credit reporting agencies in the United States), which exposed the sensitive personal information of 143 million consumers and saw hackers access names, Social Security numbers, birth dates, addresses and, in some instances, driver license numbers. The hackers also stole the credit card numbers of around 209 000 people. Consumers in the United Kingdom and Canada were also affected (Gressin, 2017).

In 2015, around 3% of all individuals across OECD countries for which data are available reported having experienced a privacy violation in the three months prior. In some countries the share can be higher – in Korea, for example, the figure is above 7% (Figure 5) (OECD, 2017a).

**Figure 5.** Individuals having experienced privacy violations in the last three months  
As a percentage of all individuals



Note: Data for Mexico refers to 2014 and is based on a different methodology.

Sources: OECD (2017a), *OECD Digital Economy Outlook 2017*, <http://dx.doi.org/10.1787/9789264276284-en>; OECD (2018d), *ICT Access and Usage by Households and Individuals* (database), <http://oe.cd/hhind>.

### Consumers are concerned over data and can perceive they have lost control

Consumer concern over how their personal data are gathered and used, and by whom, is a defining issue for the digital economy. Consumer surveys consistently show that individuals perceive digital security as a major issue, not least where there are significant risks of personal data breaches and identity theft.

Findings from the OECD survey on consumer trust in PPMs<sup>16</sup> show that believing a peer platform provider maintains the security and confidentiality of personal data is a vital building block of consumer trust in these

services, with 78% viewing this as either crucial or very important (OECD, 2017d). A Special Eurobarometer survey (European Commission, 2015a) found that European consumers' most common concerns when using the Internet for online banking or shopping relate to "someone taking or misusing personal data" (mentioned by 43% of Internet users in the European Union compared to 37% a year earlier); and the "security of online payments" (42% compared to 35% a year earlier). The same survey found 73% agreeing that they are concerned that their online personal information is not kept secure by websites. CIGI found a majority globally (55%) to be more concerned about their online privacy than they were a year ago, although concern was increasing at a slower rate than in previous years (CIGI, 2017). Among the G20 economies featured in that survey, concern was highest in India and South Africa (both 70%) and lowest in Germany (46%).

Consumers are also concerned that they are losing control over their personal data. A further *Special Eurobarometer* survey (European Commission, 2015b) found that two-thirds (67%) of EU consumers were fairly or very concerned about not having complete control over the information they provide online. A 2014 Pew Research Centre poll found 91% of Americans agreeing that consumers have lost control of their personal information and data (Madden, 2014).

Survey findings further indicate that, in addition to being concerned at what they perceive to be a loss of control, many consumers are resigned to this being a consequence of using online services. For example, the 2017 *Ipsos Global Trends* study (Ipsos, 2017) found that 72% of consumers agreed it was "inevitable" that everyone will lose some privacy in the future because of new technology. Across G20 economies, this sentiment was strongest in South Africa (84%) and Great Britain (82%) and lowest in Japan (57%) and South Korea (61%). The Special Eurobarometer survey found that a large majority of people (71%) agreed that providing personal information online is an increasing part of modern life, with 58% agreeing there is no other alternative than to provide it if they want to obtain products or services (European Commission, 2015b).

### Concerns around privacy and security risk undermining consumer trust and engagement in e-commerce

Concerns relating to privacy and security can erode trust and lead consumers to modify their online behaviours. Surveys indicate that some consumers have started to avoid using certain digital services. If left unaddressed, this is a trend that could negatively affect consumer engagement in B2C e-commerce. Around 20% of European Internet users abstained from e-banking and e-commerce in 2015 because of security concerns, including the risks of personal data misuse and of economic losses, e.g. through identity theft (Eurostat, n.d.; OECD, 2017a). When privacy concerns are taken into account the share is higher. In 2017, a quarter of EU Internet users who had not purchased online in the previous 12 months cited concerns relating to payment security or privacy as the main reason for not doing so (Eurostat, 2017).

In the United States, the 2015 US Census Bureau survey of online households reported that 63% of households were concerned about identity theft. Of this segment, 35% had refrained from conducting financial transactions online during the year prior to the survey. Similarly, of the 45% of online households concerned about credit card or banking fraud, 33% declined to buy goods or services using the Internet (Goldberg, 2016), equivalent to 15% of online households.

Notably, the G20 Digital Economy Ministerial Declaration, issued following the Düsseldorf meeting in April 2017, recognised (at para. 26) that applicable frameworks for privacy and personal data protection have to be respected, as they "are essential to strengthening confidence and trust in the digital economy" (G20, 2017).

### Wider digital security concerns

Managing digital security risk extends beyond the need for digital economy businesses to demonstrate secure stewardship of consumer data. The multitude of connected devices, including IoT technologies, via which consumers manage their transactions in the digital economy, also present a range of security risks. For

example, consumer devices can be vulnerable to cybercriminals that seek to hack, infect and remotely utilise them in order to i) exploit device users (e.g. by installing ransomware); or ii) launch external attacks on the wider web, after infecting and coordinating thousands of devices simultaneously (OECD, 2018e).

### 2.4.3 Examples of good practice

#### Certification schemes

Many governments are implementing certification schemes to increase incentives for businesses to implement effective privacy-enhancing processes. In South Korea, for instance, the Korean Communications Commission incentivises businesses to obtain a Privacy Certification by reducing fines or postponing sanctions when a certified business faces a privacy violation investigation due to a personal data breach. Similarly, in the United Kingdom, the Information Commissioner's Office is currently planning a privacy seals programme that could act as a "stamp of approval", demonstrating good privacy practice and high data protection compliance standards (OECD, 2017a).

The European Union's General Data Protection Regulation creates the possibility of implementing certification schemes that will help data controllers demonstrate compliance, and help individuals assess the level of data protection afforded by products and services. These certification schemes might be used both to demonstrate compliance with the new rules for processing operations at the EU level and to provide adequate safeguards for international data transfers (OECD, 2017a).

In some other cases, governments are promoting privacy as a business priority by emphasising the link between digital security and privacy protection. For example, Mexico's Federal Institute for Access to Public Information and Data Protection provides a table of functional equivalence between digital security standards. In collaboration with the Spanish National Cybersecurity Institute it has developed a strategic plan to help organisations improve their digital security when processing personal data (OECD, 2017a).

#### Enforcing privacy and data security

In the United States, the FTC has used its enforcement powers to address business practices that can erode consumer privacy and undermine data security. For example, in 2017 VIZIO, a major "smart" television manufacturer, agreed to pay USD 2.2 million to settle charges by the FTC and the Office of the New Jersey Attorney General. The charges alleged that VIZIO had installed software on 11 million TVs to capture second-by-second viewing data, and had done so without consumers' knowledge or consent (FTC, 2017d).

In addition, the agencies alleged that VIZIO captured IP addresses and worked with data aggregators to link specific demographic information – such as sex, age, income, marital status, household size, education level, home ownership, and household value – to the viewing data. According to the complaint, VIZIO sold this information to third parties, who used it for various purposes, including targeting advertising to consumers across devices, (FTC, 2017d; Fair, 2017b).

Alongside the payment of USD 2.2 million, the settlement ended VIZIO's unauthorised tracking, and made clear that smart TV manufacturers should obtain consumer consent before collecting and sharing television viewing information. As a result, VIZIO is required to prominently disclose its data collection and sharing practices and obtain permission from the TV owners. The company was also required to delete most of the data it had collected, and to put in place a privacy program that also checks its partners' privacy practices (Moriarty, 2017).

With regards to data security, in 2016 the FTC reached a settlement with AshleyMadison.com, a Toronto-based dating website with members from over 46 countries. The website was charged with deceiving consumers and failing to protect the account and profile information of 36 million users, in relation to a massive July 2015 data breach of its network. According to the FTC complaint, the defendants had no written

information security policy, no reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security. The settlement required the defendants to implement a comprehensive data-security program, including third-party assessments. In addition, the operators agreed to pay a total of USD 1.6 million to settle FTC and state actions (FTC, 2017c).

### 2.5 Product safety across e-commerce supply chains

#### Statement of the principle

Businesses engaging in e-commerce should not offer or advertise goods or services that pose an unreasonable risk to the health or safety of consumers; and should co-operate with competent authorities to address such risks.

#### 2.5.1 Summary of the international instruments

##### OECD Recommendation

In a number of countries, a range of unsafe products, which have been prohibited from sale or recalled from the market, remain available in e-commerce. The revised OECD *Recommendation* addresses this issue through the following provisions:

Part B on fair business, advertising and marketing practices seeks to ensure that businesses should:

- not offer, advertise or market, goods or services that pose an unreasonable risk to the health or safety of consumers (23)
- co-operate with the competent authorities when a good or a service on offer is identified as presenting such a risk (23)
- take into account the global nature of e-commerce and consider the various regulatory characteristics of the markets they target (20).

Part C on online disclosures seeks to ensure that businesses should:

- provide consumers with information describing the goods or services offered that is sufficient to enable consumers to make informed decisions regarding a transaction (31)
- depending on relevant factors, including the type of good or service, this should include information such as ... safety and health care information, and any age restrictions (32 iii and iv).

##### UN Guidelines

While the *UN Guidelines* do not address product safety in the context of e-commerce specifically, they do contain generally applicable guidance on product safety that is relevant to the sale of products online.

The General Assembly Resolution adopting the *UN Guidelines* recognises: “the importance of combating substandard, falsely labelled and counterfeit products which pose threats to the health and safety of consumers and to the environment and which also decrease consumer confidence in the marketplace.”

In introducing the objectives for the *UN Guidelines*, the preamble for Section I notes that, among other things, “consumers should have the right of access to non-hazardous products”. The general principles at Section III state a legitimate need for “the protection of consumers from hazards to their health and safety” (guideline 5 [c]).

Guidelines 16-19 at Section V, Part B are dedicated to physical safety and recommend member states adopt:

- appropriate measures to ensure that products are safe for either intended or normally foreseeable use (guideline 16)
- appropriate policies to ensure that goods produced by manufacturers are safe for either intended or normally foreseeable use (guideline 17)
- appropriate policies to ensure that if manufacturers or distributors become aware of unforeseen hazards after products are placed on the market, the relevant authorities and, as appropriate, the public are notified without delay. Member states should also consider ways of ensuring that consumers are properly informed of such hazards (guideline 18)
- policies on product recall, through which a product that poses safety risks to consumers can be replaced, modified, or substituted for another product, or, if it is not possible to do this within a reasonable period of time, the consumer should be adequately compensated (guideline 19).

Further, Section V, Part D addresses standards for the safety and quality of consumer goods and services, with guidelines 33-35 calling on member states, as appropriate, to:

- formulate or promote the elaboration and implementation of standards, voluntary and otherwise, at the national and international levels for the safety and quality of goods and services, which are publicised and reviewed periodically (guideline 33)
- raise existing standards to meet generally accepted international standards as soon as it is possible to do so (guideline 34)
- encourage and ensure the availability of facilities to test and certify the safety, quality and performance of essential consumer goods and services (guideline 35).

Under the auspices of international co-operation at Section VI, guideline 80 promotes the development or strengthening of:

*[I]nformation links regarding products which have been banned, withdrawn or severely restricted in order to enable other importing countries to protect themselves adequately against the harmful effects of such products.*

### 2.5.2 Overview of the issue

A key issue affecting consumer trust in e-commerce, especially cross-border transactions, is the number of unsafe products that are available for sale online. As noted in Section 1.5, e-commerce has put global markets at consumers' fingertips. While this is beneficial in terms of enhanced choice and convenience, it can also mean that consumers are unwittingly exposed to unsafe or hazardous products. An example of one such product being sold online is provided in Box 8.

As outlined at Section 1.3, in e-commerce, consumers are generally unable to inspect products before purchasing them. Access to safety information and warnings can be more limited than is the case in traditional retail, potentially more so when mobile devices with small screens are used.

Further, the Internet has enabled businesses to sell products via an expanded range of channels at both domestic and cross-border levels. Where in traditional retail, manufacturers distribute their goods in bulk to brick-and-mortar stores, in e-commerce, products may be distributed through online platforms, online retailers' websites, and social media. This can mean it is not always easy for consumers to identify who is actually manufacturing and delivering a product. It can also make it difficult for market surveillance authorities to detect and track unsafe products; and for authorities and manufacturers to recall and remove unsafe products from online marketplaces (OECD, 2016b).



In e-commerce, businesses selling products to consumers in a given country have traditionally been responsible for ensuring that those products are safe and have not been banned or recalled from that country's market. However, as the OECD's 2015 international product safety sweep (co-ordinated by the ACCC), highlighted, in a number of countries a range of unsafe products – which have been prohibited from sale or recalled from the market – remain available through e-commerce channels.

In this complex environment, well-equipped consumer authorities remain essential for mitigating the risks posed by unsafe products and enhancing consumer trust in the digital marketplace (OECD, 2017a). However, as the European Commission's "Notice on the market surveillance of products sold online" highlights (European Commission, 2017c), it is an environment that can pose a range of challenges for market surveillance authorities, including:

- difficulties with regard to tracing products offered for sale online and in identifying the responsible economic operators
- an increasing number of economic operators located outside the EU territory offering products for sale online to EU consumers, and a related difficulty in enforcing product safety rules within and across borders
- challenges in conducting risk assessment or safety tests due to a lack of physical access to products sold online
- lack of awareness among consumers and businesses of ways to safely buy and sell online.

### BOX 8. EXAMPLE OF AN UNSAFE PRODUCT BEING SOLD ONLINE

In 2018, European authorities ordered the distributor of a magnetic putty toy to withdraw the product from the market, after a UK Trading Standards team discovered the putty contained seven times the permitted amount of arsenic, and twice the permitted level of lead. Media reports indicated a schoolgirl had 10 times the safe limit of arsenic in her system after playing with the toy. In addition, if a child swallowed the small magnet and other metallic objects, they could attract one another and cause intestinal blockage or perforation.

The product did not carry the CE mark (which signifies compliance with European health and safety legislation) and was in breach of the requirements of the Toy Safety Directive and the relevant European standard (EN 71-1). It had been available on Amazon, eBay and Groupon all of which removed the toy once the risks were identified.

Sources: RAPEX (2018), "Alert number: A12/0227/18", <http://bit.ly/2DnsNX4>; BBC (2018), "EU arsenic warning over magnetic putty children's toy", <http://bbc.in/2FQtLjE>.

### 2.5.3 Examples of good practice

#### Product safety authorities' online market surveillance activities

In recent years, consumer product safety and partner authorities have undertaken a number of market surveillance activities and enforcement actions to detect and deter the sale of unsafe products via e-commerce. For example, the ACCC targeted 1 442 individual sites in Australia, including brick-and-mortar shops and online platforms in 2012. It inspected or tested over 16 000 consumer products, which resulted in the removal of over 100 product lines from the market (ACCC, 2014b; OECD, 2016b). Examples of the ACCC's wider activities in relation to product safety and e-commerce are provided in Box 9.

### BOX 9. ACTIONS UNDERTAKEN BY THE ACCG AND COURTS TO REMOVE UNSAFE PRODUCTS FROM E-COMMERCE

**Requiring online retailers to remove unsafe products:** in June 2013, two online retailers were found to be supplying small high-powered magnets which were prohibited from online sales in Australia. The ACCC requested that the retailers recall the products (ACCC, 2014b).

**Imposing fines:** in December 2012, a retailer selling products online and in offline stores was fined by the Australian Federal Court up to AUD 1 million (approximately USD 780 000) for selling unsafe children's nightwear which was i) flammable, and as such did not comply with mandatory safety standards; and ii) had inadequate and misleading labelling, as it did not include fire danger warnings and presented the products as a "low fire danger" (ACCC, 2014b).

**Enforceable undertakings:**<sup>1</sup> in August 2014, two online retailers provided court enforceable undertakings to the ACCC for supplying household cots that did not meet mandatory safety standards. The ACCC's testing found that infants were at risk of falling out of the cots, suffocating or becoming entrapped in them, potentially leading to death. The household cots were recalled. Court enforceable undertakings included commitments to make further attempts to notify affected consumers about the recalls, to continue offering free collection of affected cots and refunds to customers, and to implement consumer law compliance programs (ACCC, 2014c).

1. "Enforceable undertakings" are a process whereby the ACCC can choose to settle the matter administratively. The list of undertakings include: i) compensating consumers who suffered from the conduct; ii) running corrective advertisements of similar frequency and prominence to those that misled consumers; iii) paying for a company or industry trade practices compliance program; and iv) making administrative changes within the business to reduce the risk of future misleading conduct (see <http://bit.ly/2p9HuYl>).

Source: Reproduced from OECD (2016b), "Online product safety: Trends and challenges", <http://dx.doi.org/10.1787/5ilnb5q93jlt-en>.

### Organisations dedicated to online market surveillance

A number of countries have created organisations that are dedicated to e-commerce market surveillance, which have a specific duty to protect consumers from unsafe products online.

In Germany, G@ZIELT<sup>17</sup> is a centralised unit responsible for the official "control of e-commerce for food, feed, cosmetics, commodities and tobacco" (OECD, 2016b). It was established in 2013 by the Federal Office of Consumer Protection and Food Safety (BVL) and Germany's 16 Federal States (Länder), which finance the unit and direct its mission and tasks. While G@ZIELT performs centralised Internet investigations on online businesses and non-compliant products offered online, the competent authorities of the 16 Federal States carry out on-site risk-based controls of these businesses and enforce national and EU legislation. G@ZIELT gathers intelligence from various sources, such as the European Union's Food and Feed Safety Alerts and Rapid Alert System for dangerous non-food products<sup>18</sup> (hereafter RAPEX), the relevant authorities in the Federal States and from consumer complaints. The main components of the scheme are as follows (European Commission, 2015c; OECD, 2016b):

- Investigations are restricted to websites which use the German language and do not exclude delivery to Germany.
- Risk assessments<sup>17</sup> are carried out when unsafe or non-compliant products are identified.
- The competent authorities of the Federal States are informed about online traders operating from their territories.
- The competent authority of the Federal State in which the online retailer is established is informed when

unsafe or non-compliant products are offered via e-commerce websites. Necessary enforcement measures are then taken at the local level.

- Online platforms (e.g. eBay, Amazon, Alibaba), online payment operators and domain providers are asked for co-operation in the case of non-compliant offers or incorrect contact details.
- If the online retailer is established in another EU member state or third country, G@ZIELT informs the relevant competent authority of that jurisdiction.
- G@ZIELT checks periodically for products identified previously as non-compliant.

In France, the Centre de surveillance du commerce électronique (CSCE) is an agency dedicated to e-commerce market surveillance that became operational in 2001. The centre was established within the Direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF) to monitor all aspects of e-commerce, including the identification of unsafe or non-compliant products sold via the Internet in the French market. The CSCE's activities may lead to enforcement actions by one of the 122 local and regional units within the DGCCRF. CSCE's cyber inspectors receive training to identify and to trace products and operators online. In 2013, the inspectors checked 10 200 websites, 27% of which presented anomalies or instances of non-compliance (European Commission, 2015d).

### Cross-border co-operation

International co-operation between product safety authorities and with partner agencies, such as customs, is essential, given that product safety issues often have a cross-border dimension, and given the growth of cross-border transactions online. The Cooperative Engagement Framework between Canada, Mexico and the United States provides one example of a cross-border framework for sustained and increased co-operation on consumer product safety.

The following sections highlight examples of enhanced cross-border co-operation in two key areas: online sweeps and product recall databases.

### International sweeps

Online sweeps (see Section 3.4.1) have proven to be an effective way of enhancing international co-operation. During the 2015 OECD international product safety sweep, product safety authorities in 25 countries inspected three categories of goods that had been identified in their respective countries as either: i) banned and recalled products; ii) products with inadequate product labelling and safety warnings; and iii) products that did not meet voluntary or mandatory safety standards. Of the nearly 700 products inspected for the purpose of detecting banned or recalled products, 68% were available for sale online. Out of the 880 products that were inspected to detect inadequate labelling and safety warnings, 57% were not supported by adequate labelling information on relevant websites, and 22% showed incomplete labelling information. In addition, of the 136 products inspected for non-compliance with voluntary and mandatory safety standards, 54% did not comply with those standards.

A key challenge identified by the sweep is the share of unsafe products bought online from overseas, with goods banned in one country due to safety concerns, remaining accessible to buyers from another country without knowledge of the ban. Other challenges include labels and warnings in a foreign language, and products that do not meet voluntary and mandatory safety standards, which seem to be more prevalent in a cross-border context (OECD, 2016b).

### Product recall databases

Governments, businesses and consumers now enjoy greater access to tools that help detect recalled products and prevent them from reaching the market. These include the OECD's *Global Recalls* portal,<sup>19</sup> which is a

database that is available to governments, businesses and consumers alike. It brings together publicly available information on mandatory and voluntary recalls of non-food products issued by governments worldwide and also integrates recall data from the European Union's RAPEX.

RAPEX facilitates the rapid exchange of information between the national authorities of 31 countries (the EU28, plus Norway, Iceland and Liechtenstein) and the European Commission on products posing a risk to the health and safety of consumers and on the measures taken by participating countries to address those risks.

The RAPEX-China system, launched in 2006, enables information sharing on unsafe products between the European Commission (EC) and Chinese authorities. Since June 2016 this partnership has given particular emphasis to the safety of products sold online (European Commission, 2017h). Other recall databases include the Inter-American Rapid Alert System (SIAR),<sup>20</sup> which is maintained by the Organisation of American States, and the product alert database from the ASEAN Committee on Consumer Protection.<sup>21</sup>

### Co-operation between product safety authorities and online platforms

Although online platforms are, in many instances, not legally responsible for the safety of the goods supplied by third-party merchants via their sites, they have co-operated with authorities in a number of countries to help protect consumers from unsafe products.

In the United Kingdom, Hampshire County Council's Trading Standards division has established a co-operation procedure with two major e-commerce platforms. Under this procedure, Trading Standards officers receive complaints concerning unsafe products sold online through alert systems such as RAPEX. The officers can then notify the relevant platform(s) of safety issues relating to products being sold through their site and request that these be removed. In cases where a vendor selling through the platforms is found to be knowingly selling multiple non-compliant or unsafe products, including on a recurrent basis, the vendor may also be removed from the platform. This kind of public-private sector co-operation has proved efficient, as platforms are often in a better position than regulators to identify and trace sellers offering unsafe products online (European Commission, 2015d; OECD, 2016b).

In Japan the Ministry of Economy, Trade and Industry (METI) established a co-operation framework with three major e-commerce and Internet auction platforms in 2012. The framework serves to strengthen compliance with product safety laws in Japan and restrict sales of consumer products that do not meet technical standards. The framework was further expanded in 2013 to include Amazon.co.jp, which provides platform users and consumers with product recall information, when that information is provided to Amazon by METI (OECD, 2016b).

In Australia, in 2013, a foreign business was found to be supplying sky lanterns via an e-commerce platform in the country, despite a permanent prohibition to sell such products there. The ACCC and the e-commerce platform worked together to remove the lanterns from the platform (ACCC, 2014b).

In the United States, the Consumer Product Safety Commission (CPSC) brokered a good-faith co-operation agreement in 2015 with the Alibaba Group (Mozur, 2015). The following measures were to be implemented as a result of the agreement (CPSC, 2015; Howsare, 2015; OECD, 2016b):

- The establishment of a direct line enabling contacts between the US CPSC and Alibaba.
- The sharing, by the CPSC, of a list of recalled products with Alibaba, enabling it to block sales of illegal and recalled products via its platform to consumers in the United States. Measures include keyword filters to proactively block third parties using the platform to sell illegal and recalled products.
- The establishment of access points on Alibaba's B2B platforms that will direct importers of products to the United States, to US safety regulations on higher risk consumer products.

Through the RAPEX, the European Commission has stepped up its co-operation with Amazon, eBay and Alibaba to tackle potentially unsafe or non-compliant products being sold on their websites (European Commission, 2017d). In its 2017 “Commission notice on the market surveillance of products sold online”, the European Commission highlighted the role that is to be played by online platforms in preventing the sale of recalled products through their channels. This includes acting expeditiously to remove access to illegal content, such as unsafe or non-compliant products, when they become aware of such content on their platform (European Commission, 2017d). A link to the RAPEX is included in eBay’s rules and policies on product recalls, which, since March 2018, also contains a link to the OECD’s *Global Recalls* portal.<sup>22</sup>

## 2.6 Meaningful access to effective mechanisms to resolve disputes

### Statement of the principle

Consumers should be provided with meaningful access to fair and easy-to-use mechanisms to resolve disputes and obtain redress without undue cost or burden.

#### 2.6.1 Summary of the international instruments

##### OECD Recommendation

Part F of the *Recommendation* echoes the statement of the principle, advocating that:

*Consumers should be provided with meaningful access to fair, easy-to-use, transparent and effective mechanisms to resolve domestic and cross-border e-commerce disputes in a timely manner and obtain redress, as appropriate, without incurring unnecessary cost or burden. (Provision 43)*

The *Recommendation* further states that such mechanisms should include out-of-court mechanisms, such as internal complaints handling and alternative dispute resolution (ADR).

Provisions 44 and 45 expand on these mechanisms, stating that the development by business of internal complaints-handling mechanisms that enable consumers to informally resolve complaints at the earliest possible stage should be encouraged (44). With regards to ADR, the *Recommendation* states that consumers should have access to ADR mechanisms, including online systems (i.e. online dispute resolution [ODR]), with special attention given to low-value or cross-border transactions. It also states that while such mechanisms may be financially supported in a variety of ways, they should be designed to provide dispute resolution on an objective, impartial, and consistent basis (45).

Provisions 46 and 47 concern redress and specify that:

- Businesses should provide redress to consumers for the harm suffered as a consequence of goods or services which, for example, are defective, damage their devices, do not meet advertised quality criteria or where there have been delivery problems (46). This provision also encourages governments and stakeholders to consider how to provide redress to consumers for problems involving non-monetary transactions, in appropriate circumstances.
- Governments and stakeholders should work towards ensuring that consumer protection enforcement authorities and other relevant bodies, such as consumer organisations, and self-regulatory organisations that handle consumer complaints, have the ability to take action and obtain or facilitate redress for consumers, including monetary redress (47).

As noted at Section 2.2.1 on appropriate disclosures, provision 35 states that businesses should provide “information on available dispute resolution and redress options” (clause viii).

### The 2007 OECD Recommendation on Consumer Dispute Resolution and Redress

In 2007, the OECD Council adopted the *OECD Recommendation on Consumer Dispute Resolution and Redress* (hereafter the *DRR Recommendation*). The *DRR Recommendation* is aimed at addressing the practical and legal obstacles to pursuing remedies in consumer cases, whether locally or in cross-border contexts, and focuses on five priority areas for attention: i) identifying basic elements needed for effective domestic resolution and redress frameworks; ii) improving resolution of cross-border disputes; iii) enhancing the scope and effectiveness of private sector initiatives to resolve disputes; iv) developing information for monitoring developments and trends in consumer complaints; and v) improving consumer and business education and awareness on ways to avoid and handle disputes (OECD, 2007).

### UN Guidelines

The general principles at Section III include guideline 5 (g), which establishes the availability of effective consumer dispute resolution and redress as a legitimate need. Guideline 11 (f) under the principles for good business practices at Section IV addresses consumer complaints and disputes, encouraging businesses to: “make available complaints-handling mechanisms that provide consumers with expeditious, fair, transparent, inexpensive, accessible, speedy and effective dispute resolution without unnecessary cost or burden.”

Guideline 15, under “National Policies for Consumer Protection” at Section V, Part A, calls on member states to work towards “ensuring that consumer protection enforcement agencies have the necessary human and financial resources to promote effective compliance and to obtain or facilitate redress for consumers in appropriate cases.”

Section V, Part F (guidelines 37-41) is dedicated to dispute resolution and redress. Guideline 37 promotes measures to enable consumers to obtain redress through expeditious, fair, transparent, inexpensive and accessible procedures, and states that “such procedures should take particular account of the needs of vulnerable and disadvantaged consumers”. Guideline 39 states that “information on available redress and other dispute-resolving procedures should be made available to consumers” and encourages enhanced access to dispute resolution and redress mechanisms, particularly in cross-border disputes (UNCTAD, 2017a).

In addition to the *UN Guidelines*, the UN Commission on International Trade Law (UNCITRAL) released its “Technical notes on online dispute resolution” in 2016. These are designed to foster the development of ODR for use in disputes arising from cross-border low-value sales or service contracts concluded using electronic communications (UNCITRAL, 2017).

### 2.6.2 Overview of the issue

#### The case for dispute resolution and redress

When products or services fail, or fall short of consumer expectations, effective dispute resolution and redress mechanisms play a vital role in resolving and, in some instances, compensating for the detriment the consumer has experienced. Ready access to mechanisms that can provide – to paraphrase the international instruments – expeditious, fair, transparent, inexpensive, accessible, speedy and effective dispute resolution and, if required, redress, should be a core component of any consumer protection framework. Such mechanisms can help ensure that i) consumers retain the confidence to engage with individual traders, the market and enforcers; and ii) that the marketplace remains fair for all participants (UNCTAD, 2017c).

#### The added importance of dispute resolution and redress in e-commerce

The characteristics of e-commerce, where products and services are purchased untested and at a distance, mean that effective dispute resolution and redress mechanisms can play an elevated role in building consumer

trust. Indeed, research with consumers has shown that concerns over difficulties in resolving disputes satisfactorily may affect the level and types of purchases made online. For example, survey data from Eurostat shows that for EU consumers who had not shopped online in the year prior, 16% cited concerns about receiving or returning goods as a reason for not doing so (Eurostat, 2017). A consumer survey by the Fair Trading division of the Government of New South Wales, Australia, found that some respondents either did not shop online at all, or very deliberately limited the value of purchases in order to mitigate potential (and anticipated) losses (Fair Trading NSW, 2017).

Consumer wariness can be exacerbated when it comes to cross-border transactions. Here, concerns related to payment system integrity, hidden costs, fear of fraud and product quality are often more pronounced. A lack of clarity with regard to protection and avenues for redress can further aggravate these concerns (UNCTAD, 2016). As the volume of cross-border e-commerce increases, the need to establish effective mechanisms for the resolution of cross-border disputes grows in importance.

Efforts to make dispute resolution mechanisms more accessible and effective include the development and implementation of multilateral approaches for the collection and sharing of information on cross-border consumer complaints (e.g. in the case of the European Union – see Box 10); and the creation of special centres that enable consumers to file cross-border complaints in their own jurisdictions (in the case of Japan and Korea, for example). Efforts are also being made to raise consumer awareness of the possibilities that exist to resolve cross-border problems.

### The extent of consumer problems

Eurostat data for 2017 indicates that, across the European Union, more than two-thirds (69%) of consumers did not encounter any problem when buying or ordering goods or services in the 12 months prior to the survey (Eurostat, 2017). Of those that did experience problems, the most commonly cited issues included slower delivery than indicated at the time of purchase (17%); and the receipt of wrong or damaged goods or services (9%). Making complaints and seeking redress after a complaint had proved difficult for 4% of consumers.

A European Commission survey undertaken in 2016 on consumers' experiences of PPMs across the European Union found that, while most users were either satisfied or very satisfied with their experience, over half (55%) had experienced at least one problem during the 12 months prior. The two most common problems were that the product/service was either of poor quality, or not as described (European Commission, 2017a). The European Commission's study also found that almost half (46%) of consumers experiencing a problem had not sought to resolve it, primarily because the money involved was negligible, or that too much time and effort was required. Where a resolution had been sought, around two-thirds were satisfied, or very satisfied with how their complaint had been dealt with.

The OECD's 2017 survey on consumer trust in PPMs found that around a third of PPM users had, at some point in the past, experienced a problem with an item or service purchased via peer platforms.<sup>23</sup> Although a resolution was reached in the majority of cases, for many consumers the outcome was only to their partial (27%), rather than full (46%) satisfaction. For a sizeable 18% though, the matter was not resolved despite attempts to do so (OECD, 2017d). Nonetheless, the OECD survey showed that even though some consumers who had experienced a problem with a peer platform would exercise more caution in the future, very few (6%) would stop using that platform, or peer platforms more generally (3%) (OECD, 2017d).

### Approaches to dispute resolution and redress

Traditional approaches have required individuals to bring private claims before the civil courts. However, this pathway can be complex, costly, time consuming, inaccessible and disproportionate relative to the value of the dispute. Traditional approaches can thus present significant barriers for consumers, more so in the case of



cross-border disputes (UNCTAD, 2017c). Efforts to address these barriers have led to the development of ADR mechanisms, which offer easier, faster, less expensive, out-of-court solutions to disputes between consumers and vendors (UNCTAD, 2017a). In ADR systems, consumers can settle legal conflicts and disputes privately, without initiating litigation in public courts. When such procedures are mediated online, they are known as ODR. ADR procedures can take different forms and names, such as mediation, arbitration, conciliation, ombudsmen and complaints boards.

Analysis undertaken for the European Parliament highlights the particular challenges that traditional approaches pose in relation to e-commerce, particularly when cross-border transactions are involved, and notes this has led to: “conventional dispute resolution via State courts being largely ineffective and, in practice, often wholly inaccessible to the Internet consumer.” The same analysis draws a comparison between litigation in the United Kingdom, which typically takes 20 to 35 months, and ODR processes which can be completed in hours or days (Edwards and Wilson, 2007).

In addition, some countries have established governmental redress programmes, which allow consumer protection agencies, as part of the enforcement process, to obtain monetary restitution for distribution to injured consumers. Such governmental redress authority can be a critical component of an effective redress system for consumers, particularly when a detrimental practice results in relatively small injuries but is experienced by a large number of consumers. It can be an important tool for alleviating consumer injury and restoring consumer confidence in the digital marketplace.

Finally, as highlighted at Section 2.3.2, in some instances payment mechanisms can offer an effective method of consumer redress for online transactions – e.g. through credit card chargeback or electronic escrow systems.

### The challenge that digital content can pose for redress

With regards to digital content, challenges related to redress can include a lack of clarity on who is liable in the event of a problem, particularly if multiple providers are involved; and lack of access to easy and effective redress and enforcement mechanisms.

Clarity on who is liable can be particularly acute, given that consumers might not always be able to determine whether the problem originates with the content itself, the platform on which it was purchased or subscribed to (e.g. an app store, software vendor’s platform, or streaming service), the device on which the digital content product is accessed, or the service that enables access to the product (i.e. the Internet service provider [ISP]). In such a complex environment, consumers may not know who to turn to, to resolve issues. Whether the platform operator is, for example, responsible for providing consumers with product and business-related information disclosures, is an issue being explored in some jurisdictions (OECD, 2014a).

### 2.6.3 Examples of good practice

#### Effective approaches to online dispute resolution and redress

As the examples in Box 10 highlight, ODR mechanisms have been successfully developed and implemented by both government agencies and private sector actors. With regards to good practice in redress, the case study provided at Section 2.3.3, outlining the FTC’s enforcement actions against Apple, Google and Amazon on the issue of unauthorised in-app purchases by children, is equally relevant to this section. Taken together, the FTC’s actions against these companies could achieve more than USD 120 million in redress for American consumers affected by this issue (FTC, 2017b).

## BOX 10. ONLINE DISPUTE RESOLUTION IN ACTION

### Government-led initiatives

In **Brazil**, the National Consumer Secretariat created the [consumidor.gov.br](http://consumidor.gov.br) ODR portal in 2014. This public service enables disputes to be resolved online by facilitating direct exchanges between consumers and providers. Currently, 80% of complaints are resolved, with the complaint process completing in an average of seven days (UNCTAD, 2017a). Participation is only open to companies that voluntarily and formally register for the system. As of May 2018, there are 442 companies signed up to receive complaints via the platform, which has “completed” almost 1.2 million complaints from more than 900 000 registered users (Consumidor, 2018). **Mexico** launched an ODR mechanism in 2008, hosted by the Office of the Federal Prosecutor for the Consumer. This provides consumers who have purchased goods or services either online or offline, with access to a paperless and bureaucracy-free conciliation system, through which they can initiate and resolve complaints on an Internet-based virtual platform (UNCTAD, 2017a).

### EU Online Dispute Resolution platform: a regional approach

Following the passage of legislation aimed at improving and facilitating dispute resolution in cross-border online disputes, the European Commission launched the EU Online Dispute Resolution platform in February 2016. The platform aims to facilitate the online resolution of disputes between consumers and traders that have arisen from online transactions. The platform is available in 23 languages and assists consumers in submitting complaints and, along with the counterparty trader, in connecting them to approved ADR bodies.

In its first year of operation the platform handled more than 24 000 complaints, one-third of which related to a cross-border issue. Of the complaints received, 85% were automatically closed within 30 calendar days after submission (i.e. the deadline for the consumer and trader to agree on a competent ADR body). A Commission survey of consumers whose case was automatically closed revealed that, although a large number of traders did not follow through using the ODR platform, 40% of consumers had been contacted directly by the trader to solve the problem without any further progression of the complaint on the platform. (European Commission, 2017b).

### Industry initiatives: eBay

There is evidence to suggest that platform-provided ODR mechanisms can be an effective means for building and maintaining consumer trust in e-commerce. Perhaps the best-known platform dispute resolution service is eBay’s Resolution Center, which, it is claimed, has resolved “more disputes over a longer period of time than any other ODR process in the world” (Del Duca, Rule and Rimpfel, 2014). The Resolution Center handles more than 60 million e-commerce disputes annually, through a process that enables parties to resolve their problems “amicably through direct communication” (Del Duca, Rule and Rimpfel, 2014). Analysis of consumers’ behaviour following their use of the platform’s dispute resolution processes found that on average, users who reported a transaction problem and went through the ODR process increased their usage of the marketplace, regardless of the outcome. That finding included an increase in activity from buyers who had “lost” their case, albeit with their usage increasing at a slower rate than those who had “won”. Both increased their activity more than buyers who never filed a dispute in the first place (Rule, 2012).

Sources: UNCTAD (2017a), “Consumer protection in electronic commerce”, [http://unctad.org/meetings/en/SessionalDocuments/cicplpd7\\_en.pdf](http://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf); Consumidor (2018), “Indicadores”, <https://bit.ly/2i95h2T>; European Commission (2017b), “Report from the Commission to the European Parliament and the Council on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes”, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0744>; Del Duca, Rule and Rimpfel (2014), “eBay’s de facto low value high volume resolution process: Lessons and best practices for ODR systems designers”, <https://bit.ly/2KKVd1V>; Rule (2012), “Quantifying the economic benefits of effective redress: Large e-commerce data sets and the cost-benefit case for investing in dispute resolution”, <https://lawrepository.ual.edu/cgi/viewcontent.cgi?article=1005&context=lawreview>.

## 3. Regulatory framework and institutional oversight

### Introduction

This chapter focuses on the regulatory framework and the institutional oversight that is required in order to put the high-level general principles presented at Chapter 2 into practice. The starting point for policy makers engaging in this endeavour is to review and then adapt or adopt laws and regulations that recognise and respond to the risks, challenges and opportunities that e-commerce presents for consumers. At the same time, governments need to establish authorities capable of overseeing and enforcing these rules, and ensure they are equipped with the necessary legal authority and resources to do so. Section 3.1 provides a summary of what the *OECD Recommendation* and *UN Guidelines* call for in this respect. It then provides a snapshot of the progress being made in terms of countries legislating for consumer protection in e-commerce and establishing CPEAs. Self-regulation as an alternative to legislated requirements is also discussed.

Sections 3.2 to 3.4 focus specifically on the nature, role and activities of CPEAs, namely:

- the types of information gathering and enforcement powers that CPEAs require (Section 3.2)
- the need for co-operation between CPEAs at the domestic, regional and international levels, including the need for inter-disciplinary co-operation between agencies tasked with consumer, competition, data protection and sector-specific policy and enforcement (Section 3.3)
- the decision making process for consumer policy, drawing on the six-step process advocated in the OECD's 2010 *Consumer Policy Toolkit* (OECD, 2010a) (Section 3.4).

Consumer education and digital competence form the focus of the concluding section (3.5), which highlights the key role each can play in empowering consumers to better protect and advance their own interests online; and to achieve better outcomes from e-commerce.

### 3.1 Approaches to the regulatory framework

#### 3.1.1 OECD Recommendation

The *Recommendation* contains updated provisions on the essential role of consumer protection enforcement authorities and the need to enhance their ability to protect consumers in e-commerce. Part two of the *Recommendation* outlines implementation principles for the regulatory framework. It calls on governments, in co-operation with stakeholders, to achieve the purpose of the *Recommendation* by:

- reviewing and, if necessary, adopting and adapting laws protecting consumers in e-commerce, having in mind the principle of technology neutrality (53 ii)
- establishing and maintaining CPEAs that have the authority and powers to investigate and take action to protect consumers against fraudulent, misleading or unfair commercial practices and the resources and technical expertise to exercise their powers effectively (53 iii)
- encouraging the continued development of effective co-regulatory and self-regulatory mechanisms that help to enhance trust in e-commerce, including through the promotion of effective dispute resolution mechanisms (53 v).

#### 3.1.2 UN Guidelines

Under the general principles presented at Section III, guideline 4 states that member states should develop, strengthen or maintain a strong consumer protection policy, taking into account the *UN Guidelines* and relevant international agreements.

Under Section V, Part A, concerning national policies for consumer protection, guideline 14 calls upon member states to establish a set of consumer protection policies. The policies it advocates broadly align with the

general principles set out in Chapter 2 of this toolkit and Section 3.5 on consumer education. Guideline 15 then calls on member states to work towards “ensuring that consumer protection enforcement agencies have the necessary human and financial resources to promote effective compliance and to obtain or facilitate redress for consumers in appropriate cases.”

Under Section V, Part I, which addresses e-commerce specifically, guideline 64 advocates that member states should review existing consumer protection policies to accommodate the “special features of electronic commerce.”

### 3.1.3 Adoption of e-commerce specific legislation

While many countries have established a legal framework for e-commerce transactions, analysis by UNCTAD highlights how the type and extent of legislation can vary significantly by country. For example, Mexico relies on general civil law to address e-commerce issues, while France, the Russian Federation and the United States, among others, have special provisions on e-commerce within and/or in addition to their more general consumer protection laws. Some countries, including South Korea, have specific e-commerce legislation (UNCTAD, 2013). E-commerce is also dealt with in various complementary laws, such as those regulating credit card sales, competition, distance sales, telecommunications, data protection and unfair competition (UNCTAD, 2017a).

**Table 1.** Share of economies with relevant e-commerce legislation, by region, 2017 (%)

Region	Number of economies	Share in e-transaction laws	Share in consumer protection laws	Share in privacy and data protection laws	Share in cybercrime laws
<b>Developed economies</b>	42	97.6	85.7	97.6	97.6
<b>Developing economies</b>					
Africa	54	51.9	33.3	38.9	50.0
East Africa	18	44.4	22.2	27.8	61.1
Middle Africa	9	22.2	11.1	44.4	11.1
North Africa	6	83.3	33.3	33.3	83.3
Southern Africa	5	60.0	40.0	40.0	40.0
West Africa	16	62.5	56.3	50.0	50.0
Asia and Oceania	50	70.8	41.7	37.5	66.7
East Asia	4	75.0	50.0	50.0	75.0
South Asia	9	77.8	33.3	44.4	77.8
South-East Asia	11	81.8	72.7	45.5	72.7
West Asia	12	91.7	41.7	58.3	66.7
Oceania	14	42.9	14.3	7.1	42.9
Latin America and the Caribbean	33	87.9	63.6	48.5	72.7
Central America	8	87.5	87.5	37.5	62.5
South America	12	83.3	83.3	58.3	83.3
Caribbean	13	92.3	30.8	46.2	69.2
<b>Transition economies</b>	17	100.0	17.6	88.2	100.0
<b>All economies</b>	<b>196</b>	<b>77.0</b>	<b>50.0</b>	<b>57.1</b>	<b>71.9</b>

Source: UNCTAD (2017b), *Information Economy Report 2017: Digitalization, Trade & Development*, [http://unctad.org/en/PublicationsLibrary/ier2017\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf).

UNCTAD's global cyberlaw tracker maps the state of e-commerce legislation across UNCTAD's member states, focusing on the four fields identified by its research as essential for enhancing consumer confidence in e-commerce, namely: electronic transactions, consumer protection, data protection and privacy and cybercrime adoption. Table 1 shows 2017 data and highlights that, across all economies, adoption levels are lowest for laws protecting consumers online (50%) and highest (77%) for e-transaction laws (UNCTAD, 2017a).

### 3.1.4 The establishment of CPEAs

In 2017, the OECD's Committee on Consumer Policy sought to examine the extent to which CPEAs had been established, the nature of the powers available to them, and whether they were able to engage in cross-border co-operation (OECD, 2018b) (hereafter referred to as "the OECD analysis"). To support this exercise, the Committee issued a questionnaire to CPEAs in 30 countries, including 24 OECD countries and 6 partner economies.<sup>24</sup> The sample included 12 of the 19 G20 economies. The following draws on findings from this analysis.

With regard to the establishment and existence of CPEAs, the OECD analysis found that all countries surveyed have in place their own national enforcement authorities for consumer protection, although there are significant differences in consumer protection systems. Some countries have more than two competent authorities to protect consumers. In certain countries, including Germany, private enforcement bodies play an important role in enforcing consumer protection laws against businesses. Findings from the OECD analysis on the powers available to consumer protection authorities and their engagement in cross-border co-operation are referred to in subsequent sections.

### 3.1.5 A role for self-regulation

Industry self-regulation (ISR) can help to prevent harm to consumers and foster improved market functioning in a number of ways. It can, for example, provide support for businesses in overseeing the implementation of existing legal requirements. It can also go beyond legal requirements to address areas where market failures exist and no regulatory actions have been taken – perhaps because of limited resources or legal constraints (Engle, 2012). This can be particularly important in jurisdictions where legal frameworks and infrastructure may still be insufficient to provide consumers with a minimum level of protection (OECD, 2015c).

The success of ISR initiatives depends on a number of factors, including: i) the strength of the commitments made by participants; ii) the industry coverage of the ISR; iii) the extent to which participants adhere to the commitments; and iv) the consequences of not adhering to the commitments.

Advantages of ISR that are particularly relevant to the characteristics of the digital economy include:

- **More flexibility:** frequently, ISR responses to new issues can be adjusted more swiftly and easily than government regulations, which can be a time consuming, cumbersome process and may entail significant procedural hurdles (Engle, 2009).
- **Filling regulatory gaps quickly:** the rapid change that businesses and consumers encounter in markets may require existing regulations to be changed or updated frequently (OECD, 2006). However, government processes for changing regulations may take a long time. Processes overseen by industry may be more responsive and quicker. The self-regulatory process may also help establish new government regulations in the future, if required.
- **Higher technical expertise:** the higher technical expertise of industries can make them better positioned to tailor rules and guidance to their specific situations (OECD, 2015c).

These advantages suggest that ISR is well-placed to play a role in offering agile responses to emerging consumer detriments in the rapidly evolving digital economy.

ISR can also be useful at the international level as a means of addressing issues that cannot be tackled, or may be more difficult to tackle, through inter-governmental co-operation; and can help ensure that consumers are provided with a measure of protection in cross-border transactions. Many initiatives have been pursued in the standards area through the International Organization for Standardization (ISO), and ISR agreements have also been developed outside the ISO, in the areas of advertising, toys and food safety. An ISR involving the protection of consumer data flows has been adopted in the Asia Pacific Economic Cooperation (APEC) forum (OECD, 2015c).

However, ISR can also present challenges. The success of ISR agreements depends critically on the strength of their provisions, and the extent to which businesses adhere to the schemes. As events in the financial sector demonstrated in 2007-08, ISR agreements are not always successful. In particular, ISR and related initiatives that rely entirely on a voluntary approach to improve business behaviour have limitations (OECD, 2015c; OECD, 2010b).

### **3.2 Enforcement authorities and their powers**

#### **3.2.1 Powers and tools for intervention**

##### **Information gathering**

CPEAs use a wide range of information to open investigations. The OECD analysis shows that all countries surveyed use complaints from individual consumers for this purpose. Most also utilise complaints from consumer organisations, and many use media reports and complaints from businesses.

In some countries, investigations are instigated at the discretion of the CPEA, including on the basis of staff recommendations. This implies that to fulfil their responsibilities, consumer authorities need to be equipped with an appropriate number of employees with sufficient skills and expertise (see below). Some respondents to the OECD survey highlighted information from other domestic authorities and their foreign counterparts as important sources of information for opening investigations, which points to the importance of both national and international co-operation in consumer protection (OECD, 2018b).

##### **Requisite expertise**

When consumer detriment is associated with conduct in a highly technical area, or in relation to an emerging technology or disruptive business model that an authority is not yet familiar with, or that demands novel information gathering techniques or methods of analysis, this can present a challenge for CPEAs. This can be especially true in digital markets that are fast evolving and where the convergence of technologies and data blurs traditional sector boundaries and regulatory mandates. In these situations, the authority may be able to pursue the action by working with other government bodies on a cross-disciplinary basis (see Section 3.3.1), and/or by recruiting expertise on a temporary or permanent basis.

Given the ongoing transformative impact that the Internet and digital technologies are having on consumers' experiences of most sectors of the economy, it can be beneficial for authorities to establish specialist divisions that enhance their understanding of the issues that arise, and their capacity to engage with these. The FTC provides one example of an authority that has taken such steps. It has established an Office of Technology Research and Investigation (OTech), which is located at the intersection of consumer protection and new technologies. The Office conducts independent studies, evaluates new marketing practices, and provides guidance to consumers, businesses and policy makers. It also assists the FTC's consumer protection investigators and attorneys by providing technical expertise, investigative assistance, and training (FTC, n.d.).

### Powers to gather information from Internet service providers

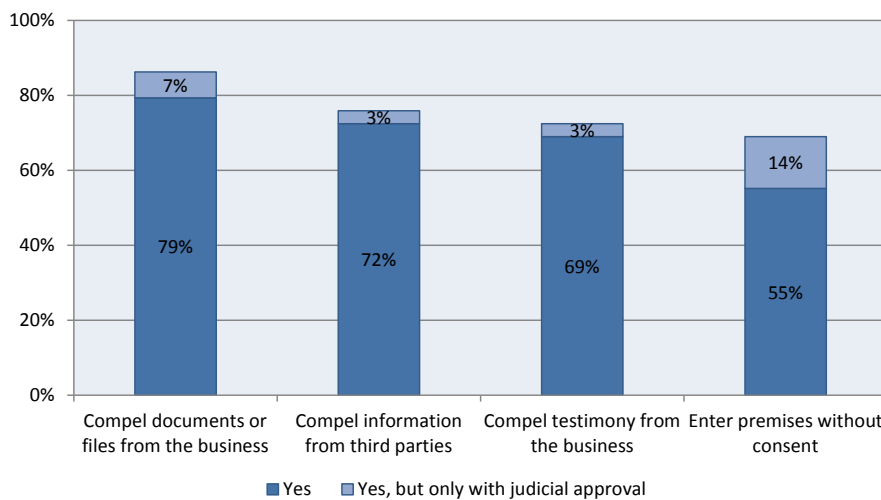
Having the statutory powers to obtain information from ISPs in support of an investigation or enforcement action, can help CPEAs mount a more efficient and effective response to online consumer detriment. The OECD’s analysis found that a legal framework granting CPEAs these powers existed in just over half of the countries it surveyed.

In some instances, including the United States and Mexico, the relevant legislation contains specific provisions that cover information gathering from ISPs. For example, in the United States, the Electronic Communications Privacy Act specifies the types of account-identifying information an agency may obtain from an Electronic Communications Service Provider, or a Remote Computing Service Provider. The Act also places limits on the types of information these providers can voluntarily provide to the government and the types of legal process the government can use to compel the provider to produce information. In other countries, consumer protection authorities are able to obtain information from ISPs or other relevant businesses through statutory information gathering powers that are not necessarily specific to ISPs. In a few instances, CPEAs have a framework or arrangements in place with ISPs, or other intermediaries, to obtain information necessary for consumer protection.

### Investigative powers

Most CPEAs can draw on some form of investigative power to support their activities. As Figure 6 highlights, most are able to compel documents or files, and many can compel testimony from the business. Moreover, CPEAs in most of the countries surveyed by the OECD reported having the power to compel information from third parties. In some countries, authorities are required to obtain a court approval in order to exercise their investigative powers against businesses engaged in fraudulent and deceptive commercial practices. For example, Canada’s consumer protection authority is required to seek approval from the court to use its investigative powers.

**Figure 6. Authorities’ investigative powers**



Note: Base = 28 agencies.

Source: OECD (2018b), “Consumer protection enforcement in a global digital marketplace”, <http://dx.doi.org/10.1787/f041eead-en>.

### 3.2.2 Enforcement and sanctions

The types of sanction available to CPEAs, and their use of them, varies widely across jurisdictions. However, a general observation is that enforcement authorities need a broad range of credible sanctions to secure compliance; and are most effective at achieving compliance when a mixture of persuasion and punishment techniques – that are proportionate to the violation in question – can be deployed (Ayres and Braithwaite, 1992). Common persuasion and punishment techniques include i) warning letters; ii) civil penalties, including

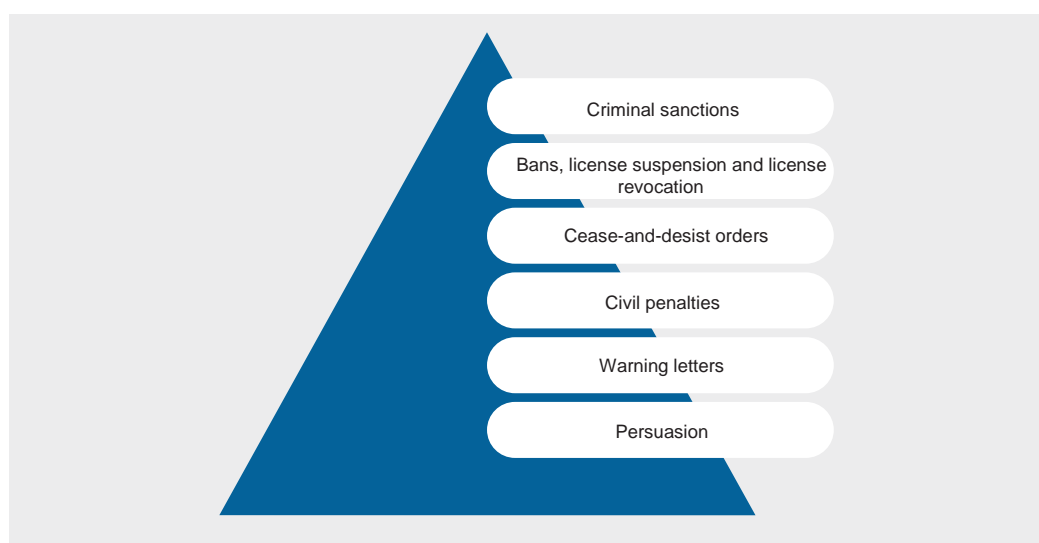


redress payments; iii) cease-and-desist orders; iv) bans, license suspensions and license revocations; and v) criminal sanctions. A summary of each is provided below.

Most regulatory action will occur at the base of the “enforcement pyramid” (Figure 7) where initial attempts to achieve compliance rely on persuasion techniques. If these fail to secure compliance, escalation up the pyramid continues until compliance is achieved. As the severity of each successive sanction increases, the likelihood it will need to be utilised decreases.

In contrast, experience shows that regulators with only one deterrence option are less effective than those that can draw on a range of sanctions. This is particularly true when the only deterrence option available is extremely severe. For example, a regulatory authority that can only issue bans may be ineffective, given that such a sanction is too severe for most problems; and given that firms will be aware that the sanction would only be used in relation to the most extraordinary offences.

**Figure 7. Enforcement pyramid**



Source: Ayres and Braithwaite (1992), *Responsive Regulation: Transcending the Deregulation Debate*.

### Warning letters

Many authorities view warning letters as a powerful and relatively cost-effective law enforcement tool. For example, in 2016, the FTC issued warning letters to 12 app developers whose apps appeared to feature Silverpush software code. Unbeknown to the user, this software could monitor a device’s microphone and listen for audio signals embedded in television advertisements. It also had the ability to produce detailed logs of content viewed. These logs could then be used for targeted advertising and analytics. The letters warned the developers that they could be in violation of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices (FTC, 2016b).

### Civil penalties (including monetary redress payments)

A civil penalty involves monetary relief that is sought by one party against another party for a wrongdoing. Civil penalties can include fines, the forfeiture of income from violations and/or a requirement to provide redress payments to consumers. Penalties should be proportionate to the harm (i.e. the consumer detriment) caused by the firm’s violations, and costs imposed on firms by any non-monetary penalties should also be included in any consideration of “optimal penalties”. In addition to punishing violators and deterring future violations, redress payments can offset consumer detriment and raise the public credibility of an enforcement authority.

### Cease-and-desist orders

A cease-and-desist order prohibits a violator from repeating the same or similar action in the future. Such orders can be structured to punish repeat offenders more harshly if, for example, penalties for repeating a violation are greater than those for an initial violation. As highlighted in Section 3.3.4, authorities within the European Union’s Consumer Protection Cooperation (CPC) network are able to call on powers to require a cessation of infringements of EU consumer law (European Commission, 2016a).

### Bans, license suspensions and license revocations

Some violations, particularly repeated violations, may warrant temporary or permanent bans on firms (or individuals) engaging in a particular line of business. For businesses or professions requiring licenses, a ban can be achieved by suspending or revoking the license.

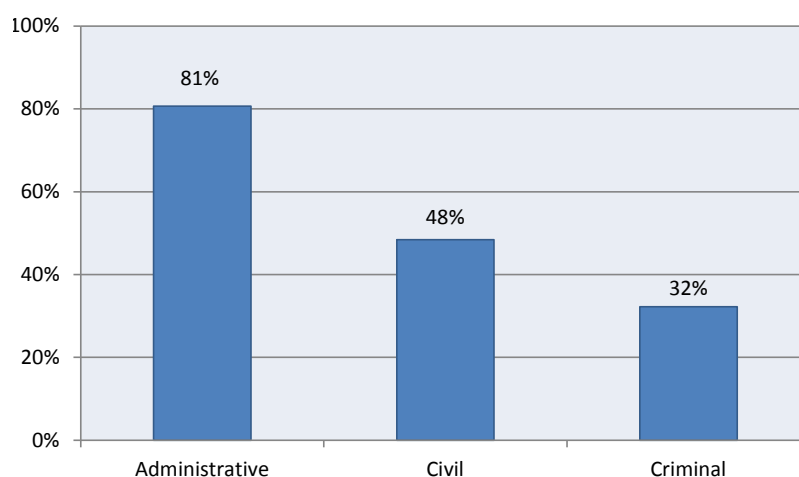
### Criminal sanctions

Some violations that cause consumer detriment may go beyond civil violations, resulting in criminal behaviour. There is no standard definition of what constitutes a criminal action as the situation varies across jurisdictions. In terms of taking action, some CPEAs have criminal enforcement powers, while others do not. In the case of the latter, co-ordination with other governmental bodies may be required if strong action is needed (OECD, 2010a).

### Enforcement powers in practice

Countries have diverse consumer protection systems, involving different laws, enforcement procedures, and roles for judicial authorities. They rely to varying extents on civil, criminal, and administrative law. The OECD analysis found a diverse range of national enforcement systems and approaches to consumer protection. As Figure 8 shows, administrative power is the most widespread type of enforcement power among the CPEAs surveyed. However, civil and criminal enforcement powers are also common.

**Figure 8.** Types of enforcement powers



Note: Base = 30 agencies.

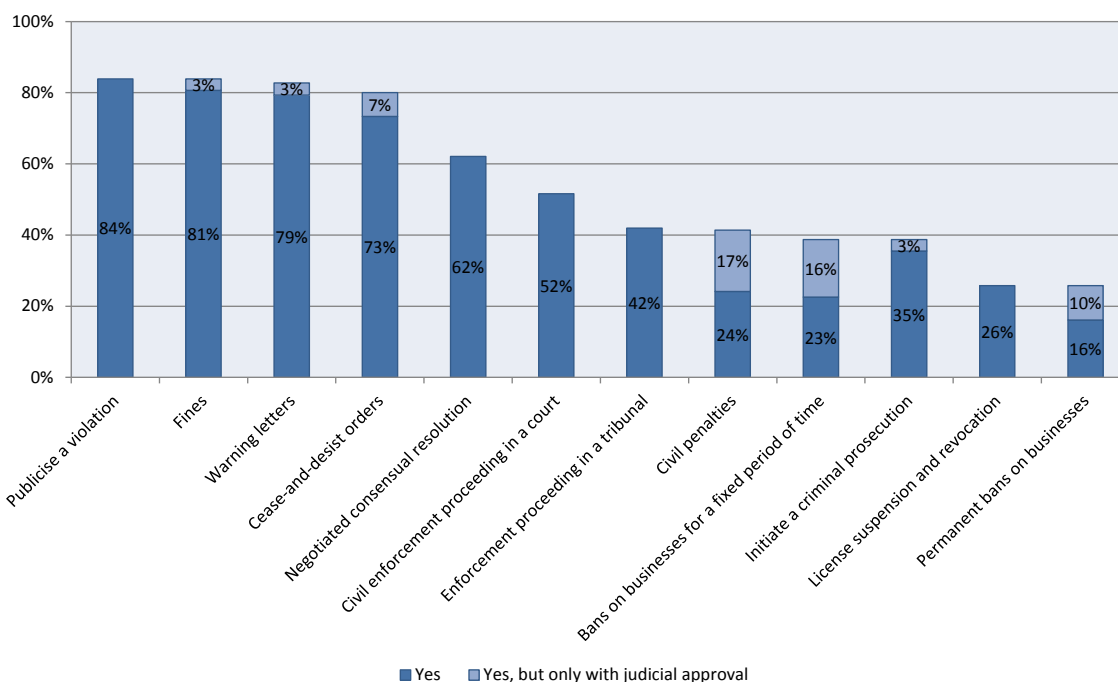
Source: OECD (2018b), “Consumer protection enforcement in a global digital marketplace”, <http://dx.doi.org/10.1787/f041eead-en>.

Many of the CPEAs surveyed had only one type of enforcement power available to them, while some CPEAs can exercise two or three types of enforcement power.

### Enforcement actions available to CPEAs

As noted at Section 3.1.1, the OECD Recommendation calls on governments to provide CPEAs with the powers necessary to take action against businesses engaged in fraudulent, misleading and/or deceptive commercial practices (provision 53 iii). As Figure 9 highlights, the OECD analysis shows that although significant differences exist, CPEAs do have a variety of tools available to them for this purpose. In some instances, the enforcement actions of some CPEAs may be subject to judicial adjudication. The most commonly available action is to publish a notice of a violation by a rogue trader, which can be undertaken in almost all instances at the discretion of the authority. Most of the CPEAs surveyed also use warning letters. There are substantial variations in the limits on the value of fines that can be levied, and on the duration of bans that can be imposed on businesses.

**Figure 9.** Type of enforcement actions available to authorities



Note: Base = 29 agencies.

Source: OECD (2018b), “Consumer protection enforcement in a global digital marketplace”, <http://dx.doi.org/10.1787/f041eead-en>.

### Sanctions and remedies available through the legal system

There is significant variation in the sanctions or remedies that are available to CPEAs through their respective legal systems. Court orders are available in most of the countries surveyed by the OECD, while a smaller majority are able to apply civil penalties and fines against businesses engaged in fraudulent and deceptive commercial practices. Additional possible sanctions or remedies reported by respondents include restitution, consignment of illicit profits, product bans, and suspension of sales.

## 3.3 Co-operation

### 3.3.1 Cross-sector co-operation

#### Convergence and data drive the need for inter-disciplinary co-operation

Data has become a vital competitive asset that plays a central role in the digital economy and sits at the core of many e-commerce business models. While the links between consumer protection and privacy (and

security) have long been clear, many of today's enforcement challenges fall within the intersection of legal frameworks for consumer protection, data protection and competition. Certain practices may violate consumer protection, privacy and competition laws simultaneously. The situation can become even more complex where the practice originates in a sector with its own regulatory framework and enforcement authority (e.g. health, communications, financial services, media, law etc.) (OECD, 2017b).

Traditionally, regulators and professionals charged with overseeing these issues come from a range of agencies, but as highlighted above, there is increasing overlap in the substantive and organisational challenges they face. This creates a need to break down the traditional "silo" approach and promote more co-ordinated governance mechanisms across these different areas. If even modest projections are correct, the growth of IoT applications and big data analytics will further elevate the role of consumer data in the digital economy. This will most likely raise new issues and different dimensions of existing challenges across consumer protection, privacy and related areas. Ultimately, silo approaches risk increasing complexity, rather than facilitating solutions that can maximise the benefits of these new developments, while minimising the potential risks (OECD, 2017b).

As a result, there is a growing need for joined-up approaches in managing the risks attached to consumer data. In designing a regulatory framework, competition law enforcers and regulatory agencies for consumer protection and data protection should share some common goals, such as the promotion of market trust, consumer choice and consumer welfare. Achieving these common goals and avoiding inconsistent approaches will necessitate strong co-operation and close dialogue between regulatory agencies (OECD, 2016c).

The United Kingdom's CMA provides one example of an authority that has recognised how the "complexity of data markets makes the role of regulators increasingly challenging" (CMA, 2015b). In order to address this challenge, the CMA is committed to working: "together with other authorities effectively, liaising and potentially working together to ensure we adopt a consistent and joined-up approach to enforcement in this area" (Box 11).

### Domestic co-operation is happening

The OECD analysis indicates that most of the CPEAs surveyed actively co-operate with other domestic authorities in the enforcement of consumer protection laws. This reflects the increased importance of regulators from various sectors better understanding the larger context of their enforcement activities. This co-operation is underpinned by legal frameworks or other arrangements and sees CPEAs collaborate with national public bodies in the fields of competition, privacy and data protection, financial services, health, environmental protection, and transport. Forms of co-operation include information sharing, collaboration on guidance for businesses, investigations, and enforcement actions – although there is variance by country (OECD, 2018b).

#### **BOX 11. THE COMPETITION & MARKETS AUTHORITY AND CROSS-SECTOR CO-OPERATION IN THE UNITED KINGDOM**

In the United Kingdom, the CMA has recognised the growing challenges of enforcement in data markets and that different types of regulation may be applicable in different circumstances. It is committed to working with other regulators to share information on new developments (e.g. technological trends and new types of products) and on complaints. Its aim is to create a robust, consistent and proportionate approach to tackling breaches of regulation, in order to create confidence in the market.

It also plays an active role in the enforcement of regulations on consumer data – working with other regulators to ensure an integrated approach to enforcement and regulation, and assessing which tools are most appropriate to tackle specific problems.

To facilitate this, the CMA has agreed Memoranda of Understanding (MOUs) with the Information Commissioner’s Office (the United Kingdom’s information and data privacy authority [ICO]), Ofcom (the communications regulator), and the Financial Conduct Authority (the financial services regulator). Ofcom has also signed a letter of understanding with the ICO setting out the basis for collaboration in areas of common enforcement responsibility.

Source: CMA (2015b), “The commercial use of consumer data: Report on the CMA’s call for information”, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/435817/The\\_commercial\\_use\\_of\\_consumer\\_data.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf).

### 3.3.2 Cross-border co-operation

#### Context and rationale

The Internet and related technologies have dramatically expanded the opportunities for B2C interactions and transactions across borders. This has created a corresponding need for deeper and more routine co-operation in cross-border enforcement. The complexities of global e-commerce supply chains also highlight the need for greater co-operation to detect and deter the sale of unsafe products to consumers (see Section 2.5). Greater co-operation across borders would also provide a more consistent regulatory environment for consumers and businesses alike – not least by helping address barriers that can diminish consumer trust in cross-border e-commerce, including difficulties consumers can face in understanding which rules apply to their transactions and what rights and responsibilities apply if a problem arises. Both the OECD and UNCTAD have dedicated considerable efforts to addressing the policy challenges inherent in making cross-border co-operation more effective (OECD, 2017b).

#### Cross-border co-operation in the international instruments

##### OECD Recommendation

Part three of the *Recommendation* sets out global co-operation principles aimed at providing effective consumer protection in the context of global e-commerce. These principles are built upon those set out in a prior OECD Recommendation, namely the *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders* (OECD, 2003). The *Recommendation* calls on governments to:

- facilitate communication, co-operation, and, where appropriate, the development and enforcement of joint initiatives at the international level among governments and stakeholders (54 i)
- improve the ability of CPEAs and other relevant authorities, as appropriate, to co-operate and co-ordinate their investigations and enforcement activities, through notification, information sharing, investigative assistance and joint actions, subject to appropriate safeguards for confidential business information or personal data (54 ii)
- utilise existing international networks and enter into bilateral and/or multilateral agreements or other arrangements as appropriate, to accomplish such co-operation (54 iii)
- continue to build consensus, both at the national and international levels, on core consumer protections to further the goals of promoting consumer welfare and enhancing consumer trust, ensuring predictability for businesses, and protecting consumers (54 iv)

- co-operate and work towards developing agreements or other arrangements for the mutual recognition and enforcement of judgements resulting from disputes between consumers and businesses, and judgements resulting from law enforcement actions taken to combat fraudulent, misleading or unfair commercial conduct (54 v)
- consider the role of applicable law and jurisdiction in enhancing consumer trust in e-commerce (54 vi).

In addition, the implementation principles set out at Part two of the *Recommendation* include a call on governments to work towards enabling CPEAs to:

*take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers, and to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against domestic consumers.* (53 iv)

### UN Guidelines

With regards to e-commerce, the General Assembly Resolution adopting the UN Guidelines considers that “certain consumer protection issues, such as applicable law and jurisdiction, may be addressed most effectively through international consultation and cooperation”.

Guideline 65 encourages member states to consider adapting and adhering to international guidelines and standards on e-commerce, as well as collaboration with other members states on cross-border implementation.

Section VI of the *UN Guidelines* addresses international co-operation. Member states are encouraged to develop mechanisms to exchange information on policies and measures related to general consumer protection (guideline 79 [a]); and to co-operate or encourage co-operation in the implementation of consumer protection policies to achieve greater results within existing resources, e.g. through common testing procedures, the exchange of consumer information and education programmes, joint training programmes and the joint elaboration of regulations (79 [b]). As noted at section 2.5.1, guideline 80 promotes the development or strengthening of information links regarding products which have been banned, withdrawn or severely restricted.

Guideline 83 encourages consumer protection enforcement agencies to co-ordinate investigations and enforcement activities. Echoing the OECD Recommendation, guideline 85 encourages member states and their consumer protection enforcement agencies to make use of existing international networks and enter into appropriate bilateral and multilateral arrangements and other initiatives to implement the UN Guidelines.

Guideline 88 calls on member states to provide their consumer protection enforcement agencies with the authority to investigate, pursue, obtain and, where appropriate, share relevant information and evidence, “particularly on matters relating to cross-border fraudulent and deceptive commercial practices.” It also states that this authority should extend to cooperation with foreign consumer protection enforcement agencies.

### Complaints indicate a need for cross-border co-operation

Consumer complaints data points to the need for greater cross-border co-operation. For example, the European Commission reports that the number of consumer complaints involving cross-border transactions has been increasing steadily. In 2015, the European Consumer Centres Network received complaints from 38 048 consumers on issues relating to cross-border purchases. Of these, 68% related to online purchases, including online shopping and Internet fraud. The European Commission estimates the detriment caused to consumers by non-compliance with basic EU consumer rules in certain cross-border online markets, and also by inefficient cross-border enforcement, amounts to EUR 770 million per year (European Parliament, 2017).

econsumer.gov is an initiative of the ICPEN (see Section 3.3.4). It allows consumers to file complaints with foreign companies and makes the complaint data available to enforcers and regulators in countries with participating agencies. It currently contains approximately 45 000 complaints.

### 3.3.3 Key elements for cross-border co-operation

The following outlines six key elements for supporting effective cross-border co-operation among and between CPEAs. Using the OECD analysis, a broad indication is given of whether the element is reflected in the existing practices of CPEAs.

#### Ability to receive complaints from consumers in other countries

The ability for CPEAs to receive and deal with complaints submitted by consumers in other countries, concerning the practices of businesses located in the CPEA's jurisdiction, is an important dimension of cross-border co-operation. The OECD analysis indicates this practice is widespread in the countries surveyed. It also indicates that some CPEAs are able to receive written consumer complaints in English, even where it is not a native language of the authority (OECD, 2018b).<sup>25</sup>

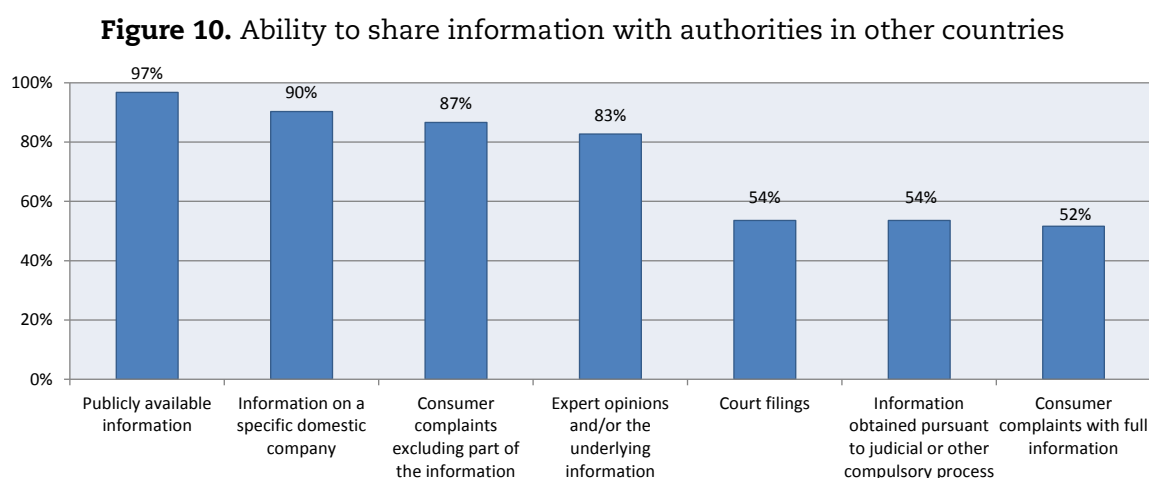
#### Notification

Effective notification procedures, whereby a CPEA can notify a foreign counterpart in instances where the former receives information on consumer detriment being caused by a business located in the latter's jurisdiction, can simplify assistance and co-operation and avoid duplication of efforts and potential disputes (OECD, 2003). The OECD analysis shows that notification procedures are commonplace (but not universal) among the CPEAs surveyed.

For some countries, notifications are based on co-operation agreements between CPEAs. For example, the FTC has notification obligations under some international co-operation agreements, such as the 1995 US-Canada agreement (OECD, 2018b). In some instances, CPEAs use existing international and regional co-operation networks such as ICPEN and the European Union's CPC network (see below) to make notifications.

#### Information sharing abilities

The ability of CPEAs to share information with foreign counterparts in a timely and effective manner is key to detecting and tackling consumer detriment arising from unsafe products and fraudulent and deceptive commercial practices across borders. The OECD analysis indicates that almost all CPEAs are able to share publicly available information, as well as information on a specific business. Many CPEAs can also share expert opinions with their counterparts. However, many CPEAs are unable to share information from non-public investigations or other confidential information. As Figure 10 highlights, issues relating to privacy, data protection and wider confidentiality considerations can prevent authorities from sharing certain classes of information (including consumer complaints and court filings) readily, if at all.



Note: Base = 30 agencies.

Source: OECD (2018b), "Consumer protection enforcement in a global digital marketplace", <http://dx.doi.org/10.1787/f041eead-en>.



### Investigative assistance

The OECD analysis indicates that, in many instances, CPEAs are able to assist in an investigation of domestic businesses by foreign counterparts. In some jurisdictions, this ability is granted by specific legal frameworks. For example, in the United States, the US Safe Web Act (2006, reauthorised 2012) enables the FTC to obtain documents, testimony, or other evidence located in the United States, to aid a foreign investigation, on the condition the request meets statutory requirements for such assistance. Under the European Union's CPC Regulation, member countries are obliged to provide assistance if they receive requests from EU counterparts. In some instances (Canada being one example), reciprocity is a condition of providing investigative assistance to foreign authorities.

### The authority to take action in cross-border cases

CPEAs having the authority to take action i) against domestic businesses engaged in fraudulent and deceptive commercial practices against consumers in other countries; and ii) against foreign businesses engaged in such practices against domestic consumers, can play a key part in ensuring effective consumer protection and enforcement across borders. In terms of taking actions against domestic businesses harming consumers in other countries, OECD analysis shows that many CPEAs are equipped to enforce laws against domestic businesses in these cases.<sup>26</sup>

### Redress

As noted at Section 2.6.1, the OECD *Recommendation* calls for consumers to be provided with dispute resolution and redress mechanisms that can help them resolve domestic *and* cross-border e-commerce disputes. The OECD analysis indicates that just over half of the countries it surveyed currently provide remedies to consumers in other countries. It also found that some countries have successfully provided remedies, such as monetary redress, to consumers from other countries in certain types of cases. For example, in Mexico, where dispute settlement is facilitated via a conciliation and arbitration procedure for consumers (OECD, 2018b).

### 3.3.4 Putting cross-border co-operation into practice

Most of the countries included in the OECD analysis have established arrangements or legal frameworks with foreign authorities to support co-operation on consumer protection and enforcement. As highlighted below, many countries also participate in international consumer protection enforcement co-operation networks, such as ICPEN. However, there is still substantial work to be done to improve cross-border enforcement co-operation on consumer issues.

#### Bilateral co-operation (Memoranda of Understanding)

A number of G20 economies have brokered bilateral agreements that facilitate cross-border co-operation on e-commerce issues. For example, the Korea Consumer Agency (KCA) has signed MOUs which set out procedures for cross-border dispute resolution with the National Consumer Affairs Centre of Japan, and the Better Business Bureau and Office of the Consumer Protection Board of Thailand (OECD, 2017a). Similarly, the ACCC has signed a MoU with the State Administration for Industry and Commerce of China, which promotes co-operation and the co-ordination of enforcement and training activities related to consumer protection (OECD, 2018b).

In 2016, the Procuraduría Federal del Consumidor (PROFECO) of Mexico signed a MoU with the Superintendency of Industry and Commerce of Colombia to strengthen co-operation on consumer rights. To achieve the objectives of this agreement, both authorities will implement co-operation activities through the exchange of experiences and information. This agreement also stresses the importance of information exchange on product safety, including results from the activities carried out by laboratories, to support decision making. PROFECO has also signed MoUs with its counterparts in Brazil, Romania, Panama and Spain.

## Regional co-operation (EU)

### The EU Consumer Protection Cooperation network

The European Union's CPC network is comprised of authorities responsible for enforcing EU consumer protection laws in EU and European Economic Area (EEA) countries. Participating authorities are obliged to provide mutual assistance. Broadly speaking, the CPC network functions as follows (European Commission, 2016a):

- An authority in the country where consumers' rights are being violated can ask its counterpart in the country where the trader is based, to take action to stop the breach. The CPC Regulation provides a list of minimum powers which each authority must have available, in order to ensure smooth co-operation. These include powers to obtain the information and evidence needed to:
  - tackle infringements within the European Union
  - conduct on-site inspections
  - require cessation or prohibition of infringements committed within the European Union
  - obtain from traders undertakings and payments into the public purse.
- Authorities can also alert each other to malpractices that could spread to other countries.
- In cases of EU-wide breaches of consumer rights, national enforcement authorities and the Commission will co-ordinate their actions to put a stop to them, especially where they concern widespread infringements with an EU dimension, which are likely to harm consumers across a large part of the Union (Council of the European Union, 2017). An example of one such co-ordinated action, concerning the terms and conditions of social media platforms, is provided in Box 12.

The CPC network has also been conducting annual Internet sweeps (see Section 3.4.1) since 2007. This is a simultaneous EU-wide screening of online platforms that seeks to identify breaches of consumer law and to then take enforcement action in a co-ordinated manner. Actions include demands to correct irregularities on the website, the imposition of fines and the closure of in-breach websites. The sweep has been conducted with different themes every year. For example, in 2016, it focused on price comparison websites, mainly in the travel sector, and found irregularities on 235 websites (two-thirds of the sites in the sweep). The network's authorities then proceeded with further investigations to establish and correct the issues identified (European Commission, 2016a).

### **BOX 12. CO-ORDINATED EU ACTION ON SOCIAL MEDIA PLATFORMS' TERMS AND CONDITIONS**

In March 2017, CPEAs within the European Union, under the leadership of the French consumer authority and with the support of the European Commission, undertook a co-ordinated action against social media platforms including Facebook, Twitter and Google+. The objective of the action was to achieve changes in the platforms' terms and conditions, so as to improve compliance with EU consumer rules. The companies were also asked to co-operate more closely with consumer authorities to remove illegal advertisements from their platforms. As a result of the action, the three platforms were asked to make a number of changes to their respective terms and conditions, to reflect that:

- EU consumers must not be deprived of rights and protections they have under their country's national legislation.
- Social media networks cannot require consumers to waive mandatory rights, such as their right to withdraw from an online purchase.
- Terms of services cannot limit or totally exclude the liability of social media networks in connection with the performance of the service.

- Sponsored content cannot be hidden, it should be identifiable as such.
- The platforms should not be able to unilaterally change their terms of service without notifying their users.
- Users must be given clear information about the rules for removal of content they have created, and the rules for termination of a contract by the platform.
- The users shall have the right to solve disputes with the companies in the country where they live.

*Note:* For an update on the outcomes of this co-ordinated action, see <http://bit.ly/2GHvoLa>.

*Sources:* European Commission (2017e), “The European Commission and member states consumer authorities ask social media companies to comply with EU consumer rules”, [http://europa.eu/rapid/press-release\\_IP-17-631\\_en.htm](http://europa.eu/rapid/press-release_IP-17-631_en.htm); OECD (2018b), “Consumer protection enforcement in a global digital marketplace”, <http://dx.doi.org/10.1787/f041eead-en>.

### International networks

The ICPEN is a membership organisation comprised of CPEAs from over 60 countries, including 14 from G20 economies. Its presidency rotates on an annual basis.

ICPEN facilitates information sharing on cross-border commercial activities that may affect consumer interests and encourages international co-operation and collaboration among consumer law enforcement agencies. It focuses on: co-ordinating co-operation on consumer protection enforcement matters; sharing information and intelligence on consumer protection trends and risks; and communicating best practice information concerning key consumer protection laws, enforcement powers and regulatory approaches to consumer protection (ICPEN, n.d.).

ICPEN is also responsible for the econsumer.gov initiative, which is an online tool that enables consumers in the countries of 35 of ICPEN’s member agencies to submit complaints online. The complaints data provides intelligence that can support consumer protection and law enforcement authorities in their investigations of, and actions against, international scams (OECD, 2017a).

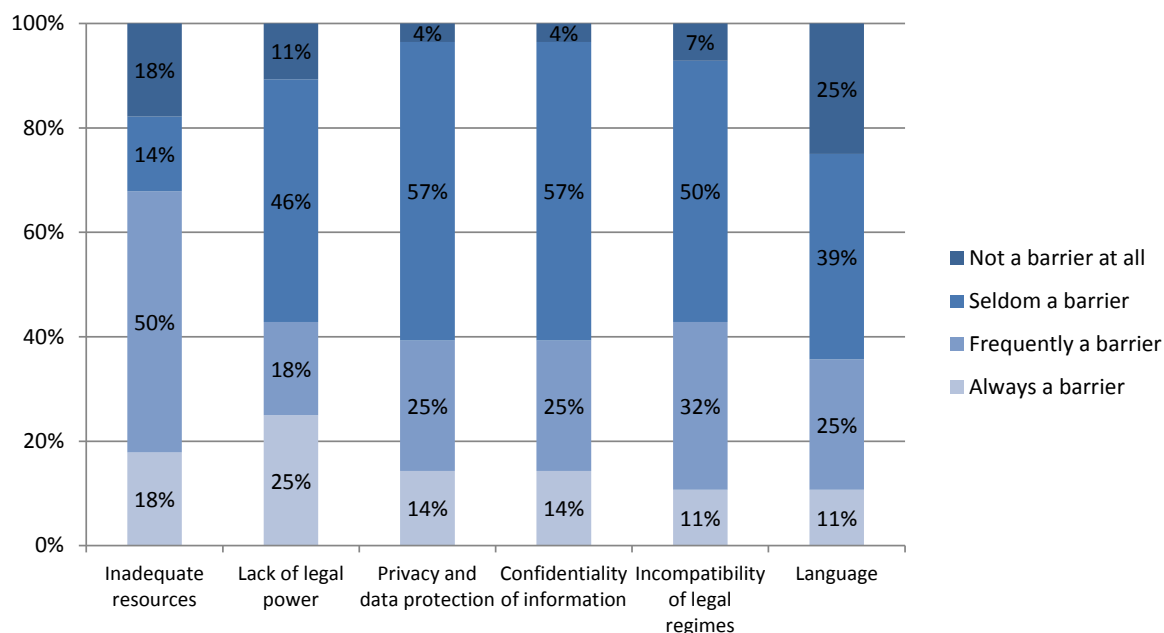
ICPEN member authorities, along with non-member enforcement bodies, conduct an annual International Internet Sweep Day, during which the participating authorities operate intensive searches to identify suspicious websites that mislead consumers. The sweep has led to a number of enforcement actions and consumer education initiatives (OECD, 2018b).

Another example of a multi-jurisdictional network is the Ibero-American Forum of Consumer Protection Agencies (FIAGC), which comprises a number of Latin American countries along with Spain and Portugal. During 2014 and 2015, member countries of FIAGC negotiated and signed a MoU enabling consumers to file complaints in their home country, if they have experienced issues with a tourism services provider in any of the member countries (OECD, 2018b).

### 3.3.5 Continued challenges to co-operation

#### Barriers to international co-operation

Despite the wide range of activities and initiatives outlined above, challenges to greater cross-border co-operation remain. These include the need to further expand the number of countries participating in cross-border co-operation; and, as the OECD analysis highlights, to ensure that CPEAs have the appropriate authority and resources to co-operate effectively, including the ability to share information with their foreign counterparts in cross-border cases (OECD, 2017b) (Figure 11).

**Figure 11.** Barriers for international co-operation in consumer protection


Note: Base = 27 agencies.

Source: OECD (2018b), "Consumer protection enforcement in a global digital marketplace", <http://dx.doi.org/10.1787/f041eead-en>.

### 3.4 The policy decision making process

#### 3.4.1 Building the evidence base (basic metrics, behavioural insights)

The work of CPEAs is focused on detecting instances where markets are falling short in meeting consumer expectations and needs, evaluating the magnitude and scope of the problems detected, and then determining whether measures should be taken to improve outcomes.

As touched on in section 3.2.1, several techniques can be used to uncover problems, ranging from assessments of complaints data to consumer surveys and independent research. However, identifying areas where problems are apparent rarely provides a sufficient basis for taking action. More in-depth analysis is often required in order to develop insights into the magnitude and scope of a problem and the nature and level of any detriment. This will be especially true in relation to novel, fast-evolving and oftentimes complex digital markets.

After summarising the relevant provisions from OECD instruments, this section – which draws on the OECD's *Consumer Policy Toolkit* (OECD, 2010a) (hereafter the *Toolkit*) – summarises a range of techniques that consumer protection agencies can utilise in gathering evidence and conducting analysis on the existence, nature and extent of consumer problems; and in determining and designing optimal responses.

#### Relevant sections of the international instruments

##### OECD Recommendation

As part of the implementation principles set out in Part two of the *Recommendation*, provision 53 states that governments should, in co-operation with stakeholders, work towards improving the evidence base for e-commerce policy making through:

- the collection and analysis of consumer complaints, surveys and other trend data
- empirical research based on the insights gained from information and behavioural economics (53 i).

### OECD Recommendation on Consumer Policy Decision Making

This *Recommendation* (OECD, 2014c), highlights key elements of the *Toolkit* (OECD, 2010a) and recommends that OECD countries develop and implement a process for policy decision making that is based on the six-step process set out in the *Toolkit* (summarised below). It also recommends that – in order to address local, national and international consumer problems – use of the policy decision making process be promoted across all levels and branches of government. OECD partner economies are also invited to adhere to this *Recommendation* and to implement it.

### Sources of information

A robust information base is essential for the effective monitoring of markets. This can draw on information that is being developed by parties other than the consumer authority, as well as information developed by the authority itself. The principal sources of such information include:

- feedback from consumers, consumer organisations, firms or other stakeholders (in the form of complaints, petitions, and related notifications)
- research carried out by consumer and other government authorities, consumer organisations, consulting groups, international organisations and networks, or other stakeholders
- reports, research, and related information available from business firms
- the media.

In addition to domestic sources, information being developed outside a country could in many instances be relevant and helpful in monitoring markets (see Section 3.3.4).

The following explores each of these information sources in turn.

### Feedback

Consumers, businesses and other stakeholders can use feedback to notify and inform governments about problems they have experienced in markets, or have become aware of. This can take various forms, including open solicitations and complaints.

Open solicitations are invitations for interested parties to suggest areas that warrant consideration by consumer authorities. These can occur through established consultative processes with stakeholders, or more informally. For example, as part of its Digital Platforms Inquiry, the ACCC has sought submissions on its Issues Paper from a range of stakeholders; and has launched an online questionnaire to solicit consumers' views and experiences in relation to the issues addressed by the Inquiry (ACCC, 2018).<sup>27</sup>

Complaints collected via formal processes are used in most countries. Individuals, groups of individuals, or other interested parties, can use these processes to bring problems to the attention of consumer authorities. Table 2 provides examples of complaints initiatives in G20 economies. In most instances, individuals are able to file complaints by phone, letter or online complaint forms (see also Box 10).

Complaints data are generally shared among authorities with responsibilities for consumer protection, and summary information is usually made available to the public. CPEAs often undertake follow-up interviews with a sample of complainants to gather additional information about the consumers affected, their complaint, the usefulness of the advice they received, and any related issues. While providing a rich source of intelligence for authorities to detect market problems, the limitations of complaints data must be kept in mind:

- Complaints may not be valid.
- There will be no complaints for problems of which consumers are unaware.

- Those who complain will represent only a subset of consumers who considered it worth their time and effort to lodge a complaint. The number of complaints may depend, for instance, on the level of consumer detriment experienced (i.e. consumers may be less likely to complain about low-value transactions).
- The complaints will be limited to consumers who know where and how to make a complaint.

**Table 2.** Examples of consumer complaint initiatives in G20 economies

<b>France</b>	Consumers can file complaints with national or local consumer organisations; some 17 of the national organisations are linked with the General Directorate for Competition Policy, Consumer Affairs and Fraud Control, which has developed a Consumer Complaints Barometer (DGCCRF, 2009). In addition, some firms have set up dispute handling mechanisms and public authorities and/or firms have set up independent sectoral ombudsmen.
<b>Korea</b>	The KCA deals with consumer counselling, redress, and dispute settlement via “Sobinet”, an integrated information processing system for consumer complaints (KCA, 2009). In 2008, the KCA dealt with about 280 000 cases of consumer complaints, over 19 000 cases of consumer redress, and about 1 400 cases of dispute settlement. These cases are summarised in an annual report and made available to the public via the KCA website.
<b>United States</b>	The FTC systematically collects and analyses consumer complaint data in its Consumer Response Center (CRC). CRC counsellors respond to consumer complaints and inquiries received by telephone, mail and e-mail. FTC staff use CRC data to spot trends and to target law enforcement and education efforts, as well as measure the impact of activities related to the FTC’s consumer protection mission. The FTC also sponsors and operates Consumer Sentinel – a secure Internet website – which law enforcement agencies use to access the database. <sup>1</sup>

1. See [www.ftc.gov/enforcement/consumer-sentinel-network](http://www.ftc.gov/enforcement/consumer-sentinel-network).

Sources: OECD (2010a), *Consumer Policy Toolkit*, <http://dx.doi.org/10.1787/9789264079663-en>.

## Research

Consumer authorities can draw on research carried out by consumer groups, businesses, academia, international organisations (such as the OECD) and consulting firms to screen markets, and/or they can undertake or commission their own research. Such research can be general, or it can be tailored to address specific needs or issues. Work can be carried out on the basis of existing information, or it could be supported by i) consumer or business surveys; ii) focus groups; and/or iii) workshops. Chapter 3 of the *Toolkit* offers guidance on different research approaches that could be utilised in support of market monitoring, along with a summary of the strengths and weaknesses of each approach.

## Internet sweeps

An Internet “sweep” is a systematic screening of websites to identify breaches of consumer law. Sweeps can be domestic in focus or undertaken as part of a co-ordinated action between co-operating CPEAs at the regional or international level (see Section 3.3.4). Sweeps are undertaken with a view to requiring contravening websites to take corrective actions. A sweep will typically focus on detecting breaches of consumer law in a specific sector (European Commission, 2016a).

## Business reports and related information

Information provided by firms can also be used to support market-monitoring activities. Disclosures of information on defective or unsafe products or litigation, for example, can provide indications of problems that require government attention. Such information may be provided voluntarily by firms (or business organisations), or it could be legally required.

## Consumer organisations and the media

Investigative journalism can be an important source of information on market performance. Consumer organisations and associations in many countries evaluate markets and products, publishing their findings in periodicals (e.g. *Choice*, in Australia<sup>28</sup>). A number also undertake and publish consumer research.

In the United Kingdom, the “super-complaint” is a formal mechanism created by Section 11(1) of the Enterprise Act 2002. It enables designated consumer organisations to submit a formal complaint – concerning “any feature, or combination of features, of a market in the United Kingdom for goods or services [that] is or appears to be significantly harming the interests of consumers” – to the relevant regulator, which is then obliged to investigate and respond accordingly (CMA, 2015c).

Governments often support or sponsor work on consumer topics. For example, in Korea the KCA has launched *Consumer Age*, a monthly consumer magazine that provides consumers with objective and reliable information on products (Korea Consumer Agency, 2009). The KCA also produces consumer information in video format for television and related media outlets.

In addition, the broadcast media (television and radio) often report on developments affecting consumers, both in the form of news stories and more in-depth programmes. For example, in Australia, *The Checkout* is a weekly consumer affairs programme that uses comedy to engage with consumers on pressing consumer issues (Australian Broadcasting Corporation, 2018). Finally, the Internet is a key information source, not least because it provides a number of channels through which consumers can readily communicate their experiences and concerns relating to markets and products; e.g. through review and ratings platforms, social media, blogs, and dedicated online communities for consumers.

## Consistency of information among sources

In theory it should be possible to use a wide range of published economic data in order to identify problem sectors and markets. This would enable, for example, data on consumer switching and data on consumer complaints to be used together when analysing a sector. To be most useful, analyses require consistent definitions across data sets, ideally at a level of aggregation that approximates the economic markets. Such consistency is difficult to achieve, as data sets are developed for a variety of purposes, and often use different definitions (OFT, 2004a).

In addition to consistency among sources, research and analysis would also be facilitated if there were harmonisation across countries. In this regard, the European Commission has adopted and is implementing a harmonised methodology for classifying and reporting consumer complaints addressed to third parties, including national authorities, consumer organisations and regulators (Chrosicki, 2015).

## Indicators

Indicators can be used to help identify areas of the economy where there are consumer issues. Indicators can be based on consumer surveys, complaints, or other data. In France, for example, a Consumer Complaints Barometer was developed in 2007, based on the complaints received by the consumer protection authority. The purpose of the barometer is to improve the ability of the government to address current and emerging issues. Complaints are organised in a way that permits authorities to analyse: i) the products and sectors which are the subject of complaints (12 sectors and 54 families of goods and services are specified); ii) the types of market operators involved (several hundred possibilities are provided); iii) the nature of the complaint (5 main domains, more than 40 themes, and close to 160 specific problems are indicated); and iv) the selling methods (Ministère de l'Économie, de l'Industrie et de l'Emploi, 2009).

In the European Union, multiple indicators are drawn together in the European Commission's “Consumer Conditions Scoreboard”, which is used to monitor markets (European Commission, n.d.). The methodology for



monitoring markets from a consumer perspective has two phases: screening and analysis. The Scoreboard provides the evidence for the screening phase and enables the identification of sectors across a market which are at risk of not functioning well in terms of economic and social outcomes; and points to where intervention may be needed. This screening of consumer markets is based on five top-level indicators: complaints, prices, switching, satisfaction, and safety. No single indicator is deemed sufficient to draw conclusions about which markets may be malfunctioning. Moreover, identifying a sector for further analysis is not to be viewed as confirmation of a malfunctioning market (OECD, 2010a).

### Market analysis

Once problem areas have been identified, consumer authorities should analyse the relevant markets in order to develop a deeper understanding of the types of problems that consumers face, and the nature and extent of the detriment.

In carrying out an analysis, information can be acquired from a variety of sources. In addition to the sources of information outlined above, consideration should be given to consulting with outside experts, developing economic models, conducting economic experiments (i.e. simulated situations using test groups) and focused investigative work. Experts' knowledge, for example, could ensure a clearer picture of the sector as well its linkages with other sectors.

Another tool that could be employed is "mystery shopping", which involves the collection of information by field workers posing as shoppers. This technique can be used to help develop more robust data and information on prices, marketing practices and firms' behaviours (Box 13). Care has to be taken, however, in the way that such shopping is carried out, so as to avoid unlawful entrapment.

### BOX 13. E-COMMERCE MYSTERY SHOPPING IN THE EUROPEAN UNION

In 2015, the European Commission conducted a large-scale mystery shopping survey (MSS) with the aim of drawing a concrete, representative picture of the way territorial restrictions are applied at different stages during the online cross-border shopping process. The specific objective of the MSS was to collect data from the consumer perspective on the prevalence and characteristics of geo-blocking across the different sectors, products and types of online retailers in the EU28.

Among other things, the MSS identified that geo-blocking practices existed in 63% of all websites assessed and that, in 2015, less than 40% of websites allowed cross-border customers to complete a purchase.

The findings were used by the European Commission to inform legislative steps to address discrimination in access to goods and services in cases where it cannot be objectively justified.

Sources: European Commission (2016b), *Mystery Shopping Survey on Territorial Restrictions and Geo-blocking in the European Digital Single Market*, <https://bit.ly/2jGkSfX>; European Commission (2017f), "Digital single market: EU negotiators agreed to end unjustified geo-blocking", [http://europa.eu/rapid/press-release\\_IP-17-4781\\_en.htm](http://europa.eu/rapid/press-release_IP-17-4781_en.htm).

Market analysis should in general seek to: i) define the nature of the observed problem in a precise manner; ii) clearly identify the market(s) affected; iii) establish the scale of the problem, both overall and for individual consumers; iv) determine whether there are vulnerable or disadvantaged groups that are disproportionately affected; and v) examine whether there is reasonable scope for designing a remedy.

In carrying out market analysis, it should be noted that the complexity and difficulty of simulating and calculating detriment<sup>29</sup> are considerable. Efforts nonetheless need to be made in order to ensure that policy makers have a robust evidence base for decision making.

### Behavioural insights

Within the consumer policy making process, behavioural insights can be especially useful in relation to three of the OECD *Toolkit's* six steps for consumer policy making (see Section 3.4.2 and Figure 12), namely:

- when defining consumer issues and their sources
- when measuring consumer detriment
- when evaluating policy options and selecting a policy action.

The following section, which is based on the OECD's *Use of Behavioural Insights in Consumer Policy* report (OECD, 2017c), summarises how policy makers might utilise behavioural insights in these three areas, and more generally.

Consumer behavioural experiments, such as laboratory experiments and randomised control trials, can help policy makers to: i) assess the effect of commercial practices on consumer behaviour and understand how consumers may behave irrationally (e.g. in response to drip pricing, or advertisements in online games); ii) choose effectively among various policy options; iii) decide on the most effective presentation of a disclosure (e.g. product labelling, terms and conditions, and price information); and iv) identify ways to increase consumer participation in measures designed to help consumers.

Some consumer authorities have utilised behavioural insights to inform their understanding of deceptive and unfair commercial practices. For example, there have been a number of enforcement actions that relate to drip pricing in online markets – a practice that can trigger behavioural biases (Box 4).

Regulations might also be designed so as to limit the ability of businesses to take advantage of certain behavioural biases. For example, the latest EU Consumer Rights Directive (2011) bans the use of pre-checked boxes for online sales, e.g. for express delivery options and travel insurance contracts when buying airline tickets (European Commission, 2014). This ban was informed by behavioural literature and its recognition of the power of default options, rather than assumptions from traditional economics that default options will not affect consumer choices (OECD, 2017c). Box 14 presents a summary of behavioural biases relevant to consumer policy making.

In terms of consumer empowerment initiatives and consumer education, some consumer authorities help consumers by providing them with tools to mitigate the effects of behavioural biases. For example, there are cases where businesses have been required to provide consumers with a simplified version of a consumer contract, in order to overcome information overload. In other cases, consumers are gaining access to their consumption data in formats that enable intermediary services to provide actionable insights based on consumption patterns and transaction histories, and support straightforward, effective decision making in complex markets.<sup>30</sup> Consumer education initiatives can also be informed by behavioural insights and be designed with behavioural biases in mind.

Applying behavioural insights to consumer policy may raise new challenges. For instance, interventions informed by behavioural insights (e.g. “nudges”) might attract criticism if these are perceived to be a form of manipulation. Consumer authorities that are new to behavioural insights may face practical challenges when starting to work in this area, e.g. if they need to dedicate time and additional resources to it, including for capacity building. These challenges, as well as the opportunities outlined above, are explored in detail in the OECD *Use of Behavioural Insights in Consumer Policy* report (OECD, 2017c). The OECD report, *Improving Online Disclosures with Behavioural Insights* (OECD, 2018c) is also relevant to this topic.

### BOX 14. EXAMPLES OF BEHAVIOURAL BIASES RELATED TO CONSUMER POLICY

**Information overload:** when faced with complex products or a bewildering array of choices, consumers may ignore possible choices, or just choose not to choose. Consumers may also rely on simple “rules of thumb” or “heuristics”.

**Default and status quo effect:** presenting one choice as a default option can induce consumers to choose that option. The power of defaults is related to the status quo effect, where consumers have a strong tendency to remain with the status quo.

**Endowment effect:** consumers often demand much more to give up an object than they would be willing to pay to acquire it: they value a good more highly when it becomes a part of their endowment. This is because consumers tend to be loss averse.

**Anchoring:** consumers “anchor” decisions around information that they think is the most important. Consumers may fail to adjust their perception of the value of an offer sufficiently, even when additional information is provided.

**Framing:** consumers are influenced by how information is presented. Presenting an option in a certain way may induce consumers to evaluate the choice from a particular reference point.

**Priming effect:** when consumers are repeatedly exposed to something – e.g. through publicity – certain attributes can play an undue role in consumer decision making. Priming can influence preferences by making certain attributes salient.

**Overconfidence:** consumers tend to think that they are more likely to experience an outcome from a given action that is better than the average expected outcome. For example, most drivers think that they are safer than the average driver.

**Hyperbolic discounting/myopia:** consumers tend to treat the present as if it were much more important than future time periods. This explains outcomes such as low retirement savings in the absence of compulsion.

**Time-inconsistency:** consumers may make choices that are not consistent across time periods due to conflicts between short-term urges and long-term interests.

**Fairness:** consumers are generally concerned that market transactions should be fair to other consumers and are often concerned about the conditions of supply (e.g. labour conditions, use of environmental resources). As a result, consumers do not always restrict their decision to the one that is in their own interest – they may consider other factors.

**Social and cultural norms:** consumers are often guided by the values, actions, and expectations of a particular society or group. For example, when people are made aware of what others are doing, it can reinforce individuals’ underlying motivations.

Source: OECD (2017c), “Use of behavioural insights in consumer policy”, <http://dx.doi.org/10.1787/c2203c35-en>.

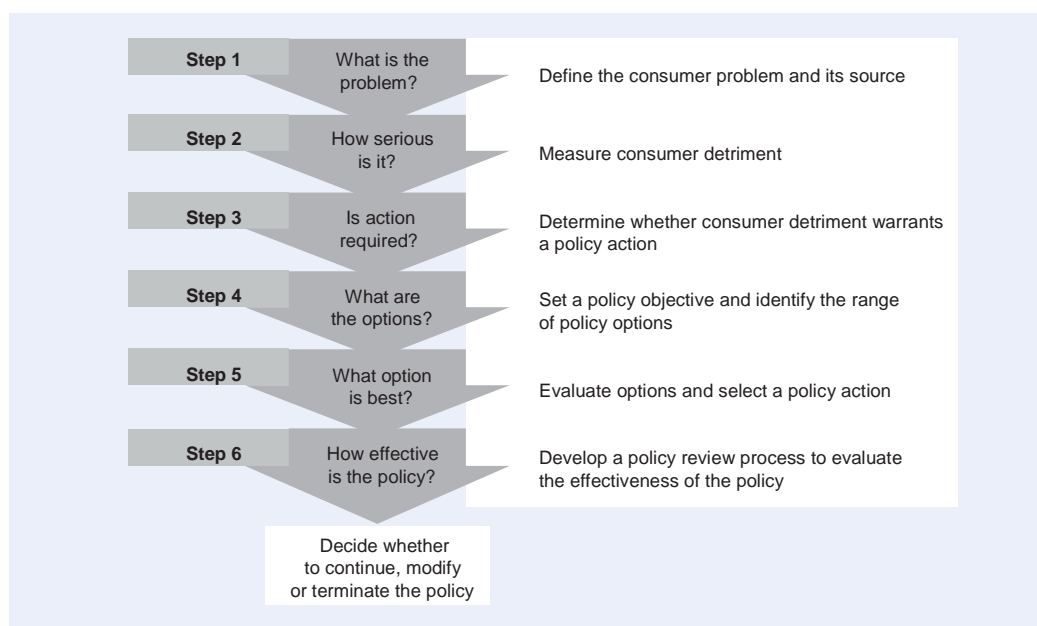
#### 3.4.2 The six-step process for consumer policy decision making

The OECD’s *Toolkit* (OECD, 2010a) presents a six-step process that provides policy makers with a framework for developing consumer policy interventions that are evidence-based and well designed (Figure 12):

- The first step – specifying the nature and source of a consumer problem – helps to identify the relevant agencies that should be involved in the policy making process.
- The second and third steps – determining the nature and magnitude of consumer detriment and determining whether policy action is warranted – provide the analytical basis for assessing whether a marketplace intervention is justified.

- The fourth step – which includes setting a policy objective and considering the full range of policy options that could be used to address a problem – helps to ensure that any policies are designed to achieve a well-defined outcome and that the full range of options (including better enforcement of existing policies) are considered.
- The fifth step – analysis of practical options (usually supported by cost-benefit examinations) – helps to ensure the selection of the most advantageous option for society. To help ensure the policy is well understood and does not have unanticipated consequences, it recommends that relevant stakeholders be consulted.
- Finally, the sixth step calls for policies to be reviewed for ongoing relevance, in order to ensure they continue to meet their objectives, or, as appropriate, that the policies be modified or eliminated (OECD, 2010a).

**Figure 12.** Consumer policy making steps



Source: OECD (2010a), *Consumer Policy Toolkit*, <http://dx.doi.org/10.1787/9789264079663-en>.

Each of the six steps is explored in greater detail below. This summary is based on the full exposition set out in the 2010 *Toolkit* itself.

### Step 1: defining the nature of the consumer problem and its source

At this stage, policy makers need to determine:

- Whether the consumer authority is the most appropriate entity to address the source of the consumer problem as a whole, or certain aspects of the problem.
- Whether the problem would be better handled by another entity. This would occur if the problem, or likely policy tools for correcting the problem, fell outside the consumer authority's mandate.
- Whether there is reasonable scope for correcting the problem at its source.
- Whether correcting the problem would conflict with other public policy objectives.

Sources of problems commonly addressed by consumer policy makers include firms' behaviours (e.g. misleading advertising), information failures, consumer's behavioural biases, and market and/or regulatory failures. If the consumer authority decides to examine a problem further, it should examine how and to what extent consumers are being harmed (Step 2).

### Step 2: measuring consumer detriment

Consumer detriment arises when market outcomes fall short of their potential, resulting in welfare losses for consumers. Identifying and measuring the nature and magnitude of consumer detriment (i.e. how consumers are being harmed and the number of, and extent to which, consumers are being harmed) is a crucial component of evidence-based policy making.

Elements of detriment include both financial and non-financial impacts, such as direct financial losses, time loss, stress and physical injury. Although quantification is often difficult, it is essential that detriment be assessed, even when it is only possible to do so in a qualitative manner. Possible sources of information for assessments include focus groups, complaints data, consumer surveys, market screening and econometric analysis (see also Section 3.4.1).

A good appreciation of consumer detriment provides consumer policy makers with the evidence to build a case, if warranted, for a market intervention (Step 3), and is also helpful in establishing an effective policy objective (Step 4).

### Step 3: determining the extent to which the detriment may warrant policy action

The decision on whether or not to intervene should consider a number of questions:

- What is the scale of consumer detriment? For example, how many consumers are affected, and what is the average detriment per consumer?
- Who is experiencing the consumer detriment? For example, disproportionate impacts on certain groups, such as children, the elderly or the socially disadvantaged, should be considered.
- What is the anticipated duration of the consumer detriment? How the detriment is likely to change over time should also be evaluated.
- What are the likely consequences of taking no policy action? The political, social and economic consequences of taking no policy action should be considered.
- Are there other substantial costs to the economy? Is the consumer problem creating detriment for other stakeholders? Is it, for example, distorting competition among firms?

Considering these factors, a consumer authority should decide whether: (i) a policy action should be considered (proceed to Step 4), (ii) more evidence is required before proceeding to policy development (return to Step 2), (iii) a better understanding of the nature and/or source of the consumer problem is necessary (return to Step 1); or (iv) no action is required, in which case the investigation would be terminated.

### Step 4: policy objectives and identifying policy options to reach objectives

#### Setting the policy objective

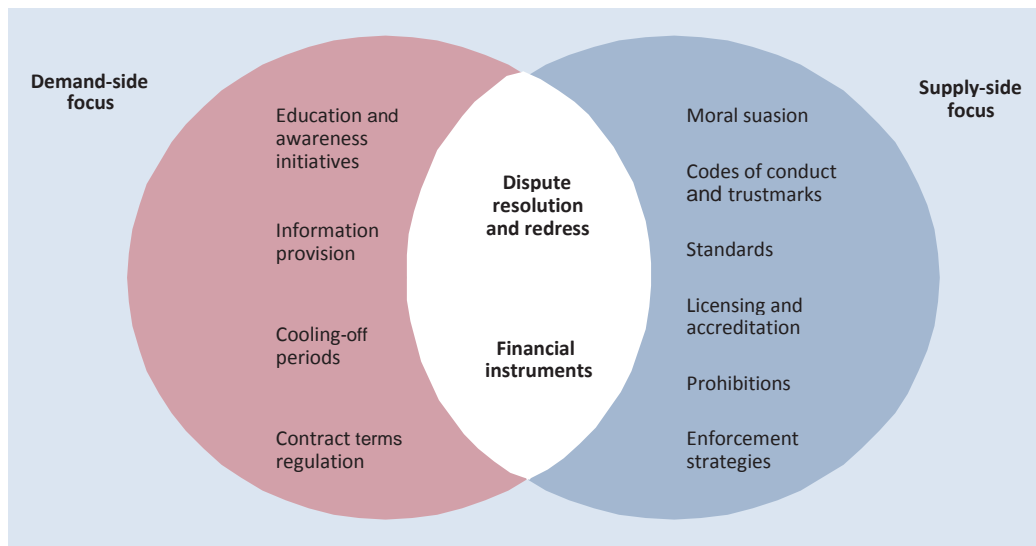
A clear policy objective should be specified, in terms of what the policy intends to achieve for consumers and the market more generally. Appropriate success indicators, targets or metrics should be determined to aid future reviews of the effectiveness of the policy (Step 6), and should be focused on market outcomes for consumers (not intermediate results). If metrics are employed, efforts should be made to establish a baseline prior to implementing a policy.

#### Identifying the range of practical policy actions

Efforts should be made to identify the full range of practical policy options (those that can be realistically implemented). These would include tools that focus on consumer empowerment and education, and those

that focus on modifying business behaviour, as well as those that have elements of both (Figure 13). Implementation of new policies and improved enforcement of existing policies should both be considered. At this stage, it is also appropriate to identify who would be responsible for implementation and enforcement, the cost of maintaining the policy, and how it would be communicated to stakeholders and the public.

**Figure 13.** Consumer policy tools to target the demand and supply side of markets



Source: OECD (2010a), *Consumer Policy Toolkit*, <http://dx.doi.org/10.1787/9789264079663-en>.

### Step 5: evaluating options and selecting optimal actions

Once policy options have been identified, the aim is to determine the most appropriate and cost-effective method for achieving the policy objective (from Step 4). In most cases, a cost-benefit analysis should be carried out, covering both quantifiable aspects and those areas where quantification may not be practicable (e.g. community values and ethical considerations). The scale and depth of an analysis should be determined based on the likely consequences of the policy under consideration. Not every action by government requires in-depth analysis. For example, an immediate temporary product ban following serious or deadly injuries to consumers would not always require a cost-benefit analysis. On the other hand, in some instances it may be worthwhile to carry out surveys, field trials and research aimed at deepening the assessment. This would likely be the case for policies that entail high costs on some stakeholders and are of a relatively permanent nature (e.g. where they are locked in by legislation).

Consultation with stakeholders, including consumer organisations, affected firms and/or industry associations, could take place at any point in time during the policy making process. However, it is particularly important to consider at this step, as it can help to ensure that options are expressed clearly and adequately address all relevant issues. It may also help reveal consequences that are not anticipated or intended by policy makers. Finally, the effects of each option on other policy areas, such as competition and the environment, should also be considered.

### Step 6: carrying out policy review and evaluation.

Regular reviews of consumer policies serve to determine if the objectives (set at Step 4) are being achieved in a cost-effective manner. The review process needs to factor in changes in the nature of the consumer problem, changes in the marketplace, and potentially unforeseen or unintended consequences of the selected policy action. The review should take place after a policy has been in operation for a reasonable period of time. Post-implementation evaluations can range from interim monitoring to full-scale reviews. The methods for carrying out reviews are similar to those used for prior assessment of expected costs and benefits. The

reviews should be used to determine whether a measure should be maintained, modified, or eliminated, whether enforcement should be strengthened, whether an alternative policy action should be considered, or whether reassessment of the nature and/or source of a problem would be beneficial (Step 1).

### 3.5 Education, awareness and digital consumer competence

Despite the benefits and opportunities inherent in e-commerce, today's consumers operate in markets that are characterised by complexity. As highlighted in Chapter 1, consumers are living through a period of dynamic change, where technological innovation transforms how they access and pay for established products and services, and gives rise to entirely new ones. These trends create the need for an enhanced consumer literacy, that can support consumers as they navigate the complexities of the digital economy, and equip them with the range of skills, knowledge and tools required to protect and advance their own interests. Initiatives to support consumer education and digital competence will play critical roles in this respect.

Consumer education can be defined as a process of developing and enhancing the skills and knowledge required to make informed and well-reasoned choices. It can help develop critical thinking and raise awareness, thereby enabling consumers to become more proactive (OECD, 2009). It is also an important vehicle for building the confidence that consumers need to engage effectively with complex markets, thereby improving market outcomes and increasing consumer welfare. In developing consumer awareness, information can be used not only to inform, but also to “nudge” consumer behaviour towards positive outcomes (OECD, 2010a).

Digital competence refers to the specific knowledge and skills that consumers need to acquire in order to access the digital economy, and to engage with it in an effective manner. This includes developing an awareness of their rights and responsibilities in relation to e-commerce. Consumers also need to know how to protect their own and others' personal information and privacy while online, and how to recognise and protect themselves from the range of risks highlighted in Chapter 2. Timely, effective education is fundamental to developing the needed competence (OECD, 2009).

#### 3.5.1 Relevant sections of the international instruments

##### OECD Recommendation

Part H of the *Recommendation* addresses education, awareness and digital competence. It calls on governments and stakeholders to work together in order to:

- Educate consumers, government officials and businesses about e-commerce to foster informed decision making; and work towards increasing business and consumer awareness of the consumer protection framework that applies to their online activities, including their respective rights and obligations, at domestic and cross-border levels (50).
- Improve consumers' digital competence through education and awareness programmes aimed at providing relevant knowledge and skills to access and use digital technology to participate in e-commerce. Such programmes should meet the needs of different groups, taking into account factors such as age, income, and literacy (51).
- Make use of all effective means to educate consumers and businesses, including innovative techniques made possible by global networks (52).

##### The UN Guidelines

The *UN Guidelines* recognise consumer education as a “legitimate need” (guideline 5 [f]). Consumer education and awareness-raising, including in relation to e-commerce, forms one of the principles establishing benchmarks



for good business practices (guideline 11 [d]); and should form part of national policies for consumer protection that member states are encouraged to establish (guideline 14 [i]).

Section V, Part G of the *UN Guidelines* is dedicated to education and information programmes, and encourages member states to:

- Develop general consumer education and information programmes that enable people to make informed choices in relation to goods and services, and raise awareness of their rights and responsibilities. Special attention should be given to the needs of vulnerable and disadvantaged consumers (guideline 42).
- Where appropriate, make consumer education an integral part of the basic curriculum of the educational system, preferably as a component of existing subjects (guideline 43).
- Treat e-commerce as an important aspect of consumer protection that should be covered by education and information programmes (guideline 44 [g]).

### 3.5.2 Consumer education

#### Education and awareness

To be effective, education and awareness strategies must go beyond addressing information asymmetries in individual transactions: they should help promote critical and active engagement by consumers generally. Indeed, awareness and education strategies work as a foundation for other consumer policy tools.

The key differences between an awareness campaign and an education initiative are their time frames and depth. Awareness campaigns are generally short-term, media-oriented actions that focus on a particular consumer issue. For example, a campaign may make consumers aware of the dangers of a newly identified unsafe good or scam. Education initiatives, on the other hand, take a long-term approach, as the focus is on developing lasting skills and/or on bringing about changes in consumer behaviour. Education initiatives may also refer to awareness campaigns. For example, school children might be taught about online topics generally, thereby raising their Internet literacy; this can then be augmented by raising students' awareness of the risks associated with data and privacy.

#### BOX 15. GENERIC AND SPECIFIC CONSUMER SKILLS

**Generic consumer skills:** in a 2004 study, the UK Office of Fair Trading identified a number of generic, transferable skills that consumers require. These include the ability to: i) research, assimilate and critically analyse information according to individual needs; ii) manage resources effectively; iii) assess risk and exercise balanced judgement in making responsible decisions; iv) communicate effectively in a wide range of consumer situations; v) solve problems where they arise; and vi) know when to seek professional advice (OFT, 2004b).

**Specific consumer skills:** these can include helping ensure consumers, or specific consumer segments, are better equipped to take advantage of the opportunities that e-commerce offers, while managing the associated risks. For example, Argentina's National Plan for Digital Inclusion includes a training programme to provide vulnerable consumers with the necessary skills, motivation, and confidence to use new technologies for their own benefit (OECD, 2018a).

Sources: OFT (2004b), "Consumer education: A strategy and framework", <https://bit.ly/2KKWV3y>; OECD (2018a), "Towards the implementation of the G20 Roadmap for Digitalisation: Skills, business dynamics and competition", [www.oecd.org/g20/OECDreport\\_Implementation\\_G20\\_Roadmap.pdf](http://www.oecd.org/g20/OECDreport_Implementation_G20_Roadmap.pdf).

The objectives of consumer awareness and education initiatives are widely cited in consumer policy literature (e.g. UNCTAD, 2017c). In general, the goals could be seen as falling into one of three categories:

- improving decision making abilities
- raising awareness of consumer rights and avenues for redress when those rights have been violated
- promoting more responsible behaviour (e.g. purchasing more environmentally sustainable products).

The goals can be pursued in either a generic or specific context (Box 15).

### Development and implementation

Careful consideration needs to be given to the purpose of an awareness or educational initiative. Is its function simply to inform consumers? Or is it to educate them in a manner that would influence their long-term behaviour? If it is the former, then the key is to communicate a succinct message to as many (relevant) consumers as possible in a timely fashion. If it is the latter, then the approach is necessarily more complex, as consumers would need to be made aware of an issue and then incentivised to become better educated about that issue.

Awareness and education initiatives can be developed and implemented by government alone or in collaboration with key stakeholders, including consumers and consumer bodies, industry, educational institutions and the media. Governments can also encourage businesses and consumer groups to conduct campaigns themselves. Joint initiatives can be particularly effective, as the partners can often communicate more effectively with target audiences, drawing on specific experiences, resources, and knowledge. Industry involvement can further strengthen messages and aid in dissemination. Working with educators, such as schools, colleges, universities and teacher associations, can also assist in effectively delivering formal education programmes.

Consumer literacy levels have important implications for consumer policy and need to be taken into account when selecting and designing policy instruments to address a problem. As events in mortgage markets in 2007-09 showed, a failure to understand the nature of financial instruments can have significant effects on individuals, with possible economy-wide implications.

### 3.5.3 Digital competence

As digitalisation reshapes economies and societies, causing a growing number of transactions and interactions to migrate to the Internet, the need for digital literacy initiatives that can equip and empower consumers with the competence required to capitalise on the opportunities, while managing the challenges, is underscored. Some countries have acted to integrate digital competence issues into their consumer education programmes, or to integrate a consumer dimension into their wider digital competence initiatives. For example, the Australian Government's Stay Smart Online initiative was established in 2006 and today provides: "topical, relevant and timely information on how home Internet users and small businesses can protect themselves from, and reduce the risk of, cyber security threats such as software vulnerabilities, online scams, malicious activities, and risky online behaviours" (Stay Smart Online, n.d.). It includes guidance on selling and shopping online, and on online banking and payments. It is also a delivery partner in Australia's annual Consumer Fraud Awareness Week.<sup>31</sup> In the United States, the FTC's, OnGuard Online web portal provides practical "how to" tips and resources on guarding against Internet fraud, securing personal computers and protecting personal information. It also offers materials for educators and parents to utilise, including online videos and games.<sup>32</sup>

The European Commission's Digital Competence Framework for Consumers (DigComp for Consumers) initiative provides an example of a regional response to the need for digitally focused consumer education. Launched in 2016 by the European Commission's Joint Research Centre and based on the Digital Competence

Framework for Citizens, DigComp for Consumers represents a “first step towards achieving a shared understanding of the competences that consumers need in the digital marketplace” (Brečko and Ferrari, 2016). It aims to clarify common goals, and to raise their visibility among stakeholders and the wider community. The initiative defines digital competence as “the competence consumers need to function actively, safely and assertively in the digital marketplace” (Brečko and Ferrari, 2016). Consumers, it is reasoned, will be in a better position to benefit from open digital markets if they acquire new knowledge, develop and practice new skills, and adopt a critical and balanced attitude to the digital world.

DigComp for Consumers is built around 14 competences that are grouped in three main areas: i) pre-purchase, ii) purchase and iii) post-purchase (Box 16). A detailed description and a non-exhaustive list of examples of the knowledge, skills, and attitudes relevant to each competence have also been developed. These aim to provide more detailed guidance on what is meant by each specific competence; and “are therefore to be used as a source of inspiration for local adaptation, or for adaptation to a specific target group or purpose” (Brečko and Ferrari, 2016). By way of illustration, Box 17 reproduces the description, and examples of the knowledge, skills and attitudes that have been developed for competence 1.1: browsing, searching and filtering information on goods and services. Expected users of the Framework are public education, consumer policy and other authorities, consumer associations, teachers and teacher training institutions, as well as private and civil society education or training actors. The initiative also aims to contribute to the implementation of the provision relating to consumers’ digital competence, that is set out in the OECD *Recommendation* (Brečko and Ferrari, 2016).

### BOX 16. COMPETENCES COVERED BY THE EUROPEAN COMMISSION'S DIGITAL COMPETENCE FRAMEWORK FOR CONSUMERS

Competence areas	Competences
(1) Pre-purchase	1.1 Browsing, searching and filtering information on goods and services 1.2 Evaluating and comparing information on goods and services 1.3 Recognising and evaluating commercial communication and advertisements 1.4 Managing digital identity and profile in the digital marketplace 1.5 Considering responsible and sustainable consumption in digital markets
(2) Purchase	2.1 Interacting in the digital marketplace to buy and sell 2.2 Participating in collaborative economy platforms 2.3 Managing payments and finances through digital means 2.4 Understanding copyrights, licences, and contracts of digital goods and services 2.5 Managing personal data and privacy 2.6 Protecting health and safety
(3) Post-purchase	3.1 Sharing information with other consumers in the digital marketplace 3.2 Asserting consumer rights in the digital marketplace 3.3 Identifying digital consumer competence gaps and limits

Source: Brečko, B. and A. Ferrari (2016), *The Digital Competence Framework for Consumers*, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfn28133enn.pdf>.

## BOX 17. ILLUSTRATION OF DESCRIPTION AND KNOWLEDGE, SKILLS, AND ATTITUDES EXAMPLES DEVELOPED FOR THE EUROPEAN COMMISSION'S DIGITAL COMPETENCE FRAMEWORK FOR CONSUMERS

### Competence 1.1 Browsing, searching and filtering information on goods and services

To search for and access information related to goods and services using digital tools. To identify and select the information needed regarding goods, services, and transaction options.

#### Knowledge examples

- recognising that search engines are not neutral, and that search results and ranking of search results of goods and services are influenced by advertising and marketing
- being aware that different search engines may give different search results for goods and services
- knowing that the Internet gives access to online shops across the world, and that it may be worthwhile to check offers in other countries/languages
- knowing about several digital tools (e.g. portals and apps) that facilitate online shopping
- realising that many companies, shops and government agencies have e-commerce and e-government services available online
- being able to name sites that sell goods at reduced prices.

#### Skills examples

- using various different search engines, changing to a different search engine to obtain better results
- filtering the search results to adjust searches
- refining information searches and selecting specific words in order to find the desired goods and services
- finding pertinent deals using digital tools and environments (e.g. by searching price comparison services)
- identifying relevant search results from search outputs
- checking search results beyond the first page.

#### Attitude examples

- being proactive in searching for information about goods and services
- valuing the positive impact that technologies have in making better-informed consumer choices
- being willing to acknowledge the limits in one's ability to process information and to resist stimuli offered by the digital marketplace.

Source: Brečko, B. and A. Ferrari (2016), *The Digital Competence Framework for Consumers*, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfn28133enn.pdf>.

## References

- 360pi (2016), “How many products does Amazon carry?”, webpage, <https://bit.ly/2J0iQmx> (accessed 28 March 2018).
- ACCC (2018), “ACCC seeking views on news and digital platforms inquiry”, media release, 26 February, Australian Competition & Consumer Commission, Canberra, <https://bit.ly/2F3Owlo> (accessed 24 March 2018).
- ACCC (2015), “Airbnb and eDreams give undertakings to ACCC for improved pricing practices”, media release, 13 October, Australian Competition & Consumer Commission, Canberra, <https://www.accc.gov.au/media-release/airbnb-and-edreams-give-undertakings-to-accc-for-improved-pricing-practices>.
- ACCC (2014a), “ACCC investigation leads to clearer ticket pricing” media release, 23 October, Australian Competition & Consumer Commission, Canberra, <http://bit.ly/1tauM9e> (accessed 18 April 2018).
- ACCC (2014b), *Consumer Product Safety Online*, Australian Competition & Consumer Commission, Canberra, <http://bit.ly/2FMdEDG> (accessed 12 March 2018).
- ACCC (2014c), “ACCC takes action against online suppliers of unsafe household cots”, news, 6 August, Australian Competition & Consumer Commission, Canberra, <http://bit.ly/2FKygMW> (accessed 12 March 2018).
- Acquisiti, A. (2010), “The economics of personal data and the economics of privacy”, Background Paper #3 for the “Joint WPISP-WPIE Roundtable on the Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines”, OECD, Paris, <https://www.oecd.org/sti/ieconomy/46968784.pdf>.
- Ahmetoglu, G. et al. (2010), “Pricing practices: Their effects on consumer behaviour and welfare”, prepared for the Office of Fair Trading.
- Airbnb (2014), “Building trust with a new review system”, webpage, <http://bit.ly/2G7iBow>.
- Australian Broadcasting Corporation (2018), “About the show”, webpage, Australian Broadcasting Corporation, [www.abc.net.au/tv/thecheckout/about](http://www.abc.net.au/tv/thecheckout/about) (accessed 4 April 2018).
- Ayres, I. and J. Braithwaite (1992), *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, Oxford.
- Bakos, Y., F. Marotta-Wurgler and D.R. Trossen (2014), “Does anyone read the fine print? Consumer attention to standard-form contracts”, *The Journal of Legal Studies*, Vol. 43/1, pp. 1-35, <https://doi.org/10.1086/674424>.
- BBC (2018), “EU arsenic warning over magnetic putty children’s toy”, news, 23 February, BBC, <http://bbc.in/2FQtLjE> (accessed 12 March 2018).
- Benartzi, S. and J. Lehrer (2017), *The Smarter Screen: Surprising Ways to Influence and Improve Online Behavior*, Penguin, New York.
- Bond, S. (2017), “Streaming revenue to surpass physical music sales this year”, *Financial Times*, 7 June, <https://www.ft.com/content/94c5cdb0-4a26-11e7-a3f4-c742b9791d43>.
- Brečko, B. and A. Ferrari (2016), *The Digital Competence Framework for Consumers*, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfn28133enn.pdf>.
- Chao, E. (2017), “How WeChat became China’s app for everything”, Fast Company, available at: <https://bit.ly/2iAZKZx> (accessed 23 March 2018).
- Chrosicki, M. (2015), “Harmonised methodology for classifying and reporting consumer complaints”, presentation, Consumer Markets Expert Group meeting 30 September 2015,

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=21197&no=9>  
(accessed 18 March 2018).

CIGI (2017), *2017 CIGI-Ipsos Global Survey on Internet Security and Trust*, Centre for International Governance Innovation, [www.cigionline.org/internet-survey](http://www.cigionline.org/internet-survey) (accessed 18 March 2018).

Civic Consulting (2011), “Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods”, Civic Consulting Survey, Final Report: Part 1: Synthesis Report, Civic Consulting, Berlin, Germany, [www.civic-consulting.de/reports/study\\_ecommerce\\_goods\\_en.pdf](http://www.civic-consulting.de/reports/study_ecommerce_goods_en.pdf).

CMA (2017), “Digital comparison tools market study: Final report”, Competition & Markets Authority, London, 26 September, <http://bit.ly/2xJgXYc> (accessed 18 April 2018).

CMA (2015a), “Online reviews and endorsements: Report on the CMA’s call for information”, Competition & Markets Authority, London.

CMA (2015b), “The commercial use of consumer data: Report on the CMA’s call for information”, Competition & Markets Authority, London, June, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/435817/The\\_commercial\\_use\\_of\\_consumer\\_data.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf).

CMA (2015c), “Guidance: What are super-complaints?”, webpage, Competition & Markets Authority, London, 7 May, <https://bit.ly/2ozZNGK> (accessed 18 March 2018).

Competition Bureau Canada (2018), “Enterprise Rent-A-Car Canada to pay a \$1 million penalty for advertising unattainable prices”, news, Competition Bureau, Gatineau, Canada.

Consumers International and VZBV (Verbraucherzentrale Bundesverband) (2017), “Building a digital world consumers can trust: Proposed recommendations from the consumer movement to the G20 member states”, Consumers International and the Federation of German Consumer Organisations, <https://bit.ly/2uhWuY0> (accessed 22 March 2018).

Consumidor (2018), “Indicadores”, webpage, <https://bit.ly/2I95h2T> (accessed 7 May 2018).

Council of the European Union (2017), “Consumer protection in the digital age: Council adopts regulation to strengthen EU-wide cooperation”, press release, 30 November, European Union, <http://bit.ly/2DjVHY5> (accessed 18 March 2018).

CPSC (13 January 2015), “Online commerce company Alibaba Group and CPSC working together on consumer safety”, CPSC On Safety blog, <http://bit.ly/2Htvbhs> (accessed 12 March 2018).

Del Duca, L.F., C. Rule and K. Rimpfel (2014), “eBay’s de facto low value high volume resolution process: Lessons and best practices for ODR systems designers”, *Arbitration Law Review*, Vol. 6: Yearbook on Mediation & Arbitration, Article 10, <https://bit.ly/2KKVd1V> (accessed 7 May 2018).

DGCCRF (2009), Unpublished communication with the OECD Secretariat.

E-commerce Foundation (2016), “Global B2C e-commerce report 2016”, E-commerce Foundation, Amsterdam, Netherlands, <https://bit.ly/2j4ixst> (accessed 29 March 2018).

Edwards, L. and C. Wilson (2007), “Redress & alternative dispute resolution in cross-border ecommerce transactions”, briefing note, IP/A/IMCO/IC/2006-206, European Parliament, Brussels, <http://www.europarl.europa.eu/document/activities/cont/201406/20140602ATT84796/20140602ATT84796EN.pdf>.

Elshout, M. et al. (2016), “Study on consumers’ attitudes towards terms and conditions (T&Cs): Final report”, report for the European Commission, Consumers, Health, Agriculture and Food Executive Agency (Chafea) on

behalf of the Directorate-General for Justice and Consumers, 22 September, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2847546](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847546).

eMarketer (2018), “Retail mcommerce sales worldwide, 2016-2021”, chart, eMarketer, <https://bit.ly/2GI7WU6> (accessed 29 March 2018).

eMarketer (2017), “Worldwide retail and ecommerce sales: eMarketer’s estimates for 2016-2021”, eMarketer, <https://bit.ly/2xx27Aa> (accessed 29 March 2018).

Engle, M.K. (2012), presentation at the FTC “Enforceable Codes of Conduct: Protecting Consumers across Borders Forum”.

Engle, M.K. (2009), Business Leadership in Consumer Protection - An OFT Conference on Self-Regulation and Industry led Compliance: An International Perspective.

EPRS (2015), “Online consumer reviews: The case of misleading or fake reviews”, briefing note, 27 October, European Union, Brussels, [www.europarl.europa.eu/RegData/etudes/BRIE/2015/571301/EPRS\\_BRI\(2015\)571301\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571301/EPRS_BRI(2015)571301_EN.pdf).

Europe Economics (2007), *An Analysis of the Issue of Consumer Detriment and the Most Appropriate Methodologies to Estimate it*, Europe Economics, London, <http://bit.ly/2F4M6Gk>.

European Commission (2017a), “Exploratory study of consumer issues in online peer-to-peer platform markets: Executive summary”, European Commission, Brussels, [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=45246](http://ec.europa.eu/newsroom/document.cfm?doc_id=45246).

European Commission (2017b), “Report from the Commission to the European Parliament and the Council on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes”, COM/2017/0744 final, European Commission, Brussels, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0744>.

European Commission (2017c), “Commission notice on the market surveillance of products sold online”, C/2017/5200, European Commission, Brussels, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017XC0801%2801%29>.

European Commission (2017d), “EU Rapid Alert System used to remove dangerous products”, news release, 16 March, European Commission, Brussels, <http://bit.ly/2FyUSwj> (accessed 18 April 2018).

European Commission (2017e), “The European Commission and member states consumer authorities ask social media companies to comply with EU consumer rules”, press release, 17 March, European Commission, Brussels, [http://europa.eu/rapid/press-release\\_IP-17-631\\_en.htm](http://europa.eu/rapid/press-release_IP-17-631_en.htm) (accessed 18 March 2018).

European Commission (2017f), “Digital single market: EU negotiators agreed to end unjustified geo-blocking”, press release, 20 November, European Commission, Brussels, [http://europa.eu/rapid/press-release\\_IP-17-4781\\_en.htm](http://europa.eu/rapid/press-release_IP-17-4781_en.htm).

European Commission (2017g), “Booking your holidays online: Commission and consumer protection authorities act on misleading travel booking websites”, press release, 7 April, European Commission, Brussels, <http://bit.ly/2oQqHJl> (accessed 18 April 2018).

European Commission (2017h), “Keeping EU consumers safe: Online marketplaces join efforts to remove dangerous products from EU market”, press release, 16 March, <https://bit.ly/2mwUqoY> (accessed 18 April 2018).

European Commission (2016a), “Consumer Protection Cooperation Network”, webpage, available at: <http://bit.ly/2lACXav> (accessed 18 March 2018).

European Commission (2016b), *Mystery Shopping Survey on Territorial Restrictions and Geo-blocking in the European Digital Single Market*, European Union, Brussels, <https://bit.ly/2jGkSfX>.



European Commission (2015a), *Special Eurobarometer 423: Cyber Security*, European Union, Brussels, <http://dx.doi.org/10.2837/411118>.

European Commission (2015b), *Special Eurobarometer 431: Data Protection*, European Union, Brussels, <http://dx.doi.org/10.2838/552336>.

European Commission (2015c), Unpublished communication with the OECD Secretariat.

European Commission (2015d), “Good practice in market surveillance activities related to non-food consumer products sold online”, European Commission, Brussels, <http://ec.europa.eu/DocsRoom/documents/8723/attachments/1/translations/en/renditions/native>.

European Commission (2015e), *Consumer Conditions Scoreboard: Consumers at Home in the Single Market, 2015 Edition*, European Union, Brussels, <http://bit.ly/2nSvISA> (accessed 29 March 2018).

European Commission (2014), “DJ Justice guidance document (Consumer Rights Directive)”, European Commission, Brussels, [https://ec.europa.eu/info/sites/info/files/crd\\_guidance\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf).

European Commission (2013a), “Consumers – Protect yourself from online fraud this festive season”, press release, 6 December, European Commission, Brussels, <https://bit.ly/2E3sH76> (accessed 28 March 2018).

European Commission (2013b), “Study on the coverage, functioning and consumer use of comparison tools and third-party verification schemes for such tools: Final report prepared by ECME Consortium”, EAHC/FWC/2013 85 07, European Commission, Brussels, [https://ec.europa.eu/info/sites/info/files/final\\_report\\_study\\_on\\_comparison\\_tools\\_2013\\_en.pdf](https://ec.europa.eu/info/sites/info/files/final_report_study_on_comparison_tools_2013_en.pdf).

European Commission (n.d.), “Consumer scoreboards”, webpage, <https://bit.ly/2oIreNT> (accessed 18 March 2018).

European Parliament (2017), “Consumer protection cooperation”, Briefing EU Legislation in Progress, European Parliament, Brussels, [www.europarl.europa.eu/RegData/etudes/BRIE/2016/586676/EPRS\\_BRI\(2016\)586676\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586676/EPRS_BRI(2016)586676_EN.pdf).

Eurostat (2017), “E-commerce statistics for individuals”, Eurostat, <http://bit.ly/1VR9CKT> (accessed 12 March 2018).

Eurostat (n.d.), *Digital Economy and Society* (database), Eurostat, <http://bit.ly/2Ilw6ld> (accessed 6 May 2018).

Fair, L. (2017a), “Three FTC actions of interest to influencers”, Federal Trade Commission Business Blog, 7 September, <https://bit.ly/2i7HGHX> (accessed 26 March 2018).

Fair, L. (2017b), “What Vizio was doing behind the TV screen”, Federal Trade Commission Business Blog, 6 February, <https://bit.ly/2jVD73J> (accessed 7 May 2018).

Fair Trading (2017), Online Shopping Survey Report May 2017, NSW Government, <https://bit.ly/2GoBISU> (accessed 24 March 2018).

FTC (2017a) “CSGO Lotto Owners Settle FTC’s First-Ever Complaint Against Individual Social Media Influencers” press release, September 7, Federal Trade Commission, Washington, DC, <https://bit.ly/2xS06zX>

FTC (2017b), “FTC, Amazon to withdraw appeals, paving way for consumer refunds related to children’s unauthorized in-app charges” press release, 4 April, Federal Trade Commission, Washington, DC, <http://bit.ly/2nMGt5Z>.

FTC (2017c), “Privacy & Data Security Update (2016)”, Federal Trade Commission, Washington, DC, <https://bit.ly/2vxiW6i>.

FTC (2017d), “VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users’ Consent” press release, 6 February, Federal Trade Commission, Washington, DC, <https://bit.ly/2keuQUy>.

FTC (2016a), “Big Data – A Tool for Inclusion or Exclusion?”, Federal Trade Commission, Washington, DC, <https://bit.ly/1n52gG6> (accessed 3 May 2018).

FTC (2016b), “FTC issues warning letters to app developers using ‘Silverpush’ code”, press release, 17 March, Federal Trade Commission, Washington, DC, <https://bit.ly/1pqLrGx> (accessed 24 March 2018).

FTC (2014a), “FTC approves final order in case about Apple Inc. charging for kids’ in-app purchases without parental consent”, press release, 27 March, Federal Trade Commission, Washington, DC, <http://bit.ly/2HryqWt>.

FTC (2014b), “FTC approves final order in case about Google billing for kids’ in-app charges without parental consent”, press release, 5 December, Federal Trade Commission, Washington, DC, <http://bit.ly/2Ik3ybl>.

FTC (2013), “.com Disclosures – How to make effective disclosures in digital advertising”, Federal Trade Commission, Washington, DC, <https://bit.ly/1W32GM8>.

FTC (n.d.), “Office of Technology Research and Investigation”, webpage, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation> (accessed 18 March 2018).

G20 (2017), “G20 Digital Economy Ministerial Declaration: Shaping digitalisation for an interconnected world”, German Federal Ministry for Economic Affairs and Energy, Düsseldorf, Germany, [http://unctad.org/meetings/es/Contribution/dtl\\_eWeek2017c02-G20\\_en.pdf](http://unctad.org/meetings/es/Contribution/dtl_eWeek2017c02-G20_en.pdf).

Gefen, D. and D. Straub (2004), “Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-products and e-services”, *Omega: The International Journal of Management Science*, Vol. 32/6, pp. 407-424, <https://doi.org/10.1016/j.omega.2004.01.006>.

Goldberg, R. (13 May 2016), “Lack of trust in Internet privacy and security may deter economic and other online activities”, National Telecommunications and Information Administration blog, <http://bit.ly/27jfxS>.

Government of Australia (2006), *The Australian Guidelines for Electronic Commerce*, March 2006, Commonwealth of Australia, Canberra, <https://bit.ly/2HaZD4j> (accessed 18 April 2018).

Gressin, S. (2017), “The Equifax data breach: What to do”, Federal Trade Commission, Washington, DC, 8 September, <http://bit.ly/2wNHFPb>.

Grothaus, M. (2015), “You’ll never guess what the first thing ever sold on the Internet was”, Fast Company, 26 November, <https://bit.ly/2INB7TU> (accessed 23 March 2018).

Hill, K. (2012), “How Target figured out a teen girl was pregnant before her father did”, *Forbes*, 16 February, <https://bit.ly/2FZ7T6B> (accessed 23 March 2018).

Howsare, M. (2015), “CPSC and e-commerce giant Alibaba ink deal to block sale of recalled products to U.S. consumers”, Mintz Levin, 14 January, <http://bit.ly/2tOycHh> (accessed 12 March 2018).

ICPEN (2016), “Online reviews & endorsements: ICPEN guidelines for review administrators”, International Consumer Protection and Enforcement Network, <https://www.icpen.org/sites/default/files/2017-06/ICPEN-ORE-Guidelines%20for%20Review%20Administrators-JUN2016.pdf>.

ICPEN (n.d.), “What we do”, webpage, International Consumer Protection and Enforcement Network, [www.icpen.org/what-we-do](http://www.icpen.org/what-we-do) (accessed 18 March 2018).

- Institute for Consumer Policy (2017), “Indicators of consumer protection and empowerment in the digital world: Results and recommendations of a feasibility study”, Institute for Consumer Policy, Berlin, Germany, 15 March, <https://www.bmjv.de/G20/DE/ConsumerSummit/documents/Downloads/Studie.pdf?blob=publicationFile&v=1>.
- IPC (2018), IPC Cross-border E-commerce Shopper Survey 2017, International Post Corporation, Brussels, <https://www.ipc.be/en/knowledge-centre/e-commerce/cross-border-e-commerce-shopper-survey>.
- Ipsos (2017), “Ipsos Global Trends: 8. Online behaviour”, Ipsos, <https://bit.ly/2HJJnUK> (accessed 18 April 2018).
- Ipsos (2014), “Global trends 2014: Navigating the new”, Ipsos, <http://bit.ly/2FEMmiA> (accessed 18 April 2018).
- Kemp, S. (30 January 2018), “Digital in 2018: Essential insights into Internet, social media, mobile and e-commerce use around the world”, WE ARE SOCIAL blog, <https://wearesocial.com/blog/2018/01/global-digital-report-2018>.
- KCA (Korea Consumer Agency) (2009), Unpublished communication with the OECD Secretariat.
- Koske, I. et al. (2014c), “The Internet economy: Regulatory challenges and practices”, *OECD Economics Department Working Papers*, No. 1171, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5jxszm7x2qmr-en>.
- Lally, A. and R. Goldberg (2017), “Upper court underwhelmed by overstock”, 7 June, <http://bit.ly/2IeSAnJ> (accessed 18 April 2018).
- Lanier, J. (2013), *Who Owns the Future?*, Simon & Schuster, New York.
- Madden, M. (2014), “Public perceptions of privacy and security in the post-Snowden era”, Pew Research Center, Washington, DC, 12 November, [www.pewinternet.org/2014/11/12/public-privacy-perceptions/](http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/).
- Marotta-Wurgler, F. (2012), “Does contract disclosure matter?”, *Journal of Institutional and Theoretical Economics*, Vol. 168/1, pp. 94-119, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2736521](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736521).
- Meeker, M. (2015), “Internet trends 2015: Code conference”, 27 May, [www.kpcb.com/blog/2015-internet-trends](http://www.kpcb.com/blog/2015-internet-trends) (accessed 29 March 2018).
- Ministère de l’Économie, de l’Industrie et de l’Emploi (2009), “Constitution du baromètre des plaintes des consommateurs”, webpage (in French), <https://bit.ly/2qHUtCm> (accessed 18 April 2018).
- Mohammed, R. (2017), “How retailers use personalized prices to test what you’re willing to pay”, *Harvard Business Review*, 20 October, <https://bit.ly/2qWuYjh> (accessed 26 March 2018).
- Moriarty, K (February 6, 2017), “VIZIO Settlement: Smart TVs should not track your shows without your O.K.”, Federal Trade Commission Consumer Information Blog, <https://bit.ly/2HjtBik> (accessed 6 May 2018).
- Moynihan, D.O. (2014), “California court imposes \$6.8 million in civil penalties against Overstock.com for allegedly deceptive price comparisons”, 23 April, <http://bit.ly/2Ftpkbr> (accessed 18 April 2018).
- Mozur, P. (2015), “Alibaba will help curb export of recalled items”, *New York Times*, 13 January, <http://nyti.ms/2FJaSPR> (accessed 12 March 2018).
- NTS (2018), “Six sentenced for large copycat website fraud”, news, 6 March, National Trading Standards, <http://bit.ly/2p1gRFR> (accessed 18 April 2018).
- OECD (forthcoming), “A dynamic e-commerce landscape: Developments, trends and business models”, *OECD Digital Economy Papers*, OECD, Paris.
- OECD (2018a), “Towards the implementation of the G20 Roadmap for Digitalisation: Skills, business dynamics and competition”, OECD, Paris, [www.oecd.org/g20/OECDreport\\_Implementation\\_G20\\_Roadmap.pdf](http://www.oecd.org/g20/OECDreport_Implementation_G20_Roadmap.pdf).

- OECD (2018b), “Consumer protection enforcement in a global digital marketplace”, *OECD Digital Economy Papers*, No. 266, OECD Publishing, Paris, <http://dx.doi.org/10.1787/f041eead-en>.
- OECD (2018c), “Improving online disclosures with behavioural insights”, *OECD Digital Economy Papers*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/39026ff4-en>.
- OECD (2018d), *ICT Access and Usage by Households and Individuals* (database), <http://oe.cd/hhind> (accessed April 2018).
- OECD (2018e), “Consumer policy and the smart home”, *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, <http://dx.doi.org/10.1787/e124c34a-en>.
- OECD (2017a), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264276284-en>.
- OECD (2017b), “Key issues for digital transformation in the G20”, report prepared for a joint G20 German Presidency/OECD Conference, OECD, Paris, <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>.
- OECD (2017c), “Use of behavioural insights in consumer policy”, *OECD Science, Technology and Industry Policy Papers*, No. 36, OECD Publishing, Paris, <http://dx.doi.org/10.1787/c2203c35-en>.
- OECD (2017d), “Trust in peer platform markets: Consumer survey findings”, *OECD Digital Economy Papers*, No. 263, OECD Publishing, Paris, <http://dx.doi.org/10.1787/1a893b58-en>.
- OECD (2016a), *Consumer Protection in E-commerce: OECD Recommendation*, OECD, Paris, <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>.
- OECD (2016b), “Online product safety: Trends and challenges”, *OECD Digital Economy Papers*, No. 261, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5jlnb5q93jlt-en>.
- OECD (2016c), “Big data: Bringing competition policy to the digital era”, OECD, Paris, [www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm](http://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm).
- OECD (2016d), “OECD Ministerial Declaration on the digital economy: Innovation, growth and social prosperity”, OECD, Paris, [www.oecd.org/internet/oecd-digital-economy-ministerial-declaration.htm](http://www.oecd.org/internet/oecd-digital-economy-ministerial-declaration.htm) (accessed 28 March 2018).
- OECD (2015a), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264229358-en>.
- OECD (2015b), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD, Paris, [www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf](http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf).
- OECD (2015c), “Industry self-regulation: Role and use in supporting consumer interests”, *OECD Digital Economy Papers*, No. 247, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5js4k1fjqkwh-en>.
- OECD (2014a), “Consumer policy guidance on intangible digital content products”, *OECD Digital Economy Papers*, No. 241, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5jxvbrjq3gg6-en>.
- OECD (2014b), “Consumer policy guidance on mobile and online payments”, *OECD Digital Economy Papers*, No. 236, OECD Publishing, Paris, <http://dx.doi.org/10.1787/5jz432cl1ns7-en>.
- OECD (2014c), *OECD Recommendation on Consumer Policy Decision Making*, OECD, Paris, <https://www.oecd.org/sti/consumer/Toolkit-recommendation-booklet.pdf>.
- OECD (2013), “OECD Guidelines governing the protection of privacy and transborder flows of personal data”, Ch. 1 in *The OECD Privacy Framework*, OECD, Paris, [http://oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).

- OECD (2011), *OECD Guide to Measuring the Information Society 2011*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264113541-en>.
- OECD (2010a), *Consumer Policy Toolkit*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264079663-en>.
- OECD (2010b), *Annual Report on the OECD Guidelines for Multinational Enterprises 2010: Corporate Responsibility: Reinforcing a Unique Instrument*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/mne-2010-en>.
- OECD (2009), "Consumer education: Policy recommendations of the OECD'S Committee on Consumer Policy", DSTI/CP(2009)5/FINAL, OECD, Paris, [www.oecd.org/sti/consumer/44110333.pdf](http://www.oecd.org/sti/consumer/44110333.pdf).
- OECD (2007), *OECD Recommendation on Consumer Dispute Resolution and Redress*, OECD, Paris, [www.oecd.org/internet/consumer/38960101.pdf](http://www.oecd.org/internet/consumer/38960101.pdf).
- OECD (2006), "Alternatives to traditional regulation", OECD, Paris.
- OECD (2003), *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264103573-en-fr>.
- OECD (2001), "Business-to-consumer e-commerce statistics", OECD, Paris, [www.oecd.org/internet/consumer/1887351.pdf](http://www.oecd.org/internet/consumer/1887351.pdf).
- OECD (1999a), *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris, [www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm](http://www.oecd.org/sti/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm).
- OECD (1999b), "FAQs on the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce", OECD, Paris, [www.oecd.org/sti/consumer/2091663.pdf](http://www.oecd.org/sti/consumer/2091663.pdf) (accessed 23 March 2018).
- OFT (2013), "Price comparison websites: Trust, choice and consumer empowerment in online markets", Office of Fair Trading, London.
- OFT (2012), "Airlines to scrap debit card surcharges following OFT enforcement action", Office of Fair Trading, London.
- OFT (2004a), "Empirical indicators for market investigations: Summary and conclusions", Office of Fair Trading, London.
- OFT (2004b), "Consumer education: A strategy and framework", Office of Fair Trading, London, <https://bit.ly/2KKWV3y> (accessed 8 May 2018).
- Orlando, J. (2014), "The app trap: How children spend thousands online", *The Conversation*, 19 February, <http://bit.ly/1cXFkg7>.
- RAPEX (2018), "Alert number: A12/0227/18", Rapid Alert System for dangerous non-food products, European Commission, <http://bit.ly/2DnsNX4> (accessed 12 March 2018).
- Rule, C. (2012), "Quantifying the economic benefits of effective redress: Large e-commerce data sets and the cost-benefit case for investing in dispute resolution", *University of Arkansas at Little Rock Law Review*, Vol. 34/4, pp. 767-777, <https://lawrepository.ualr.edu/cgi/viewcontent.cgi?article=1005&context=lawreview>.
- Sauro, J. (2011), "Do users read license agreements?", 11 January, *MeasuringU*, <https://measuringu.com/eula>.
- ScrapeHero (2018), "How many products does Amazon sell?", *ScrapeHero*, January, <https://bit.ly/2n6kadm> (accessed 28 March 2018).
- Shirky, C. (2009), *Here Comes Everybody: The Power of Organizing Without Organizations*, Penguin Books, London.
- Smith, A. and M. Anderson (2016), "Online shopping & e-commerce", *Pew Research Center*, December, <https://pewrsr.ch/2kuSaAM> (accessed 29 March 2018).

- Smithers, R. (2011), “Terms and conditions: Not reading the small print can mean big problems”, *The Guardian*, London, <https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems>.
- Soper, S. and J. Cao (2015), “The trouble with online customer reviews”, Bloomberg, 23 December, <https://bloom.bg/2tvGPe8> (accessed 18 April 2018).
- Stay Smart Online (n.d.), “About us”, webpage, [www.staysmartonline.gov.au/about-us](http://www.staysmartonline.gov.au/about-us) (accessed 24 March 2018).
- Terms & Conditions May Apply (2013), Film, directed by C. Hoback. Hyrax Films, <http://tacma.net/> (accessed 6 May 2018).
- Trenholm, R. (2013), “Eight-year-olds worst for running up shock in-app charges”, cnet, 8 May, <http://cnet.co/2p9NFvU>.
- UNCITRAL (2017), “Technical notes on online dispute resolution”, United Nations Commission on International Trade Law, Vienna, [www.uncitral.org/pdf/english/texts/odr/V1700382\\_English\\_Technical\\_Notes\\_on\\_ODR.pdf](http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf).
- UNCTAD (2017a), “Consumer protection in electronic commerce”, United Nations Conference on Trade and Development, Geneva, [http://unctad.org/meetings/en/SessionalDocuments/cicplpd7\\_en.pdf](http://unctad.org/meetings/en/SessionalDocuments/cicplpd7_en.pdf).
- UNCTAD (2017b), *Information Economy Report 2017: Digitalization, Trade & Development*, United Nations, Geneva, [http://unctad.org/en/PublicationsLibrary/ier2017\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf).
- UNCTAD (2017c), *Manual on Consumer Protection*, United Nations, New York and Geneva, <https://bit.ly/2HOREzK> (accessed 4 May 2018).
- UNCTAD (2016), “Data protection regulations and international data flows: Implications for trade and development”, United Nations, New York and Geneva, [http://unctad.org/en/PublicationsLibrary/dtlstict2016d1\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf).
- UNCTAD (2015), *Information Economy Report: Unlocking the Potential of E-commerce for Developing Countries*, United Nations, New York and Geneva, [http://unctad.org/en/PublicationsLibrary/ier2015\\_en.pdf](http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf) (accessed 28 March 2018).
- UNCTAD (2013), “Implementation report on the United Nations Guidelines on Consumer Protection (1985-2013)”, TD/B/C.I/CLP/23, United Nations Conference on Trade and Development, Geneva, [http://unctad.org/meetings/en/SessionalDocuments/cicplpd23\\_en.pdf](http://unctad.org/meetings/en/SessionalDocuments/cicplpd23_en.pdf).
- United Nations (2015), “Resolution adopted by the General Assembly on 22 December 2015: 70/186 Consumer protection”, comprising the *United Nations Guidelines for Consumer Protection* as an annex, United Nations, New York, <https://bit.ly/293y1M6> (accessed 8 May 2018)
- US Department of Commerce (2018), “Quarterly retail e-commerce sales, 3rd quarter 2017”, US Census Bureau News, 16 February, <https://bit.ly/2GFnWpD> (accessed 29 March 2018).
- Walmart (n.d.), “Our retail divisions”, webpage, [https://corporate.walmart.com/\\_news\\_/news-archive/2005/01/07/our-retail-divisions](https://corporate.walmart.com/_news_/news-archive/2005/01/07/our-retail-divisions).
- Wigglesworth, R. (2017), “Will the death of US retail be the next big short?”, *Financial Times*, 16 July, <https://www.ft.com/content/d34ad3a6-5fd3-11e7-91a7-502f7ee26895>.
- Xia, L. and K.B. Monroe (2004), “Price partitioning on the Internet”, *Journal of Interactive Marketing*, Vol. 18/4, pp. 63-73, <https://doi.org/10.1002/dir.20017>.



## Notes

1. The *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* (OECD, 1999a)
2. For further information concerning the summit, see [www.bmju.de/G20/EN/ConsumerSummit/G20\\_node.html](http://www.bmju.de/G20/EN/ConsumerSummit/G20_node.html).
3. VZBV is the Federation of German Consumer Organisations (see <http://en.vzbv.de/>).
4. Separately, the OECD has produced *Towards the Implementation of the G20 Roadmap for Digitalisation: Skills, Business Dynamics and Competition* (OECD, 2018a). It has also produced the report *Key Issues for Digital Transformation in the G20* (OECD, 2017b).
5. “Impersonal” is used here to describe consumers’ experience of the transaction process. However, it is recognised that greater personalisation can be a key benefit of e-commerce for consumers – both in the increased opportunities it presents for consumers to customise products and services to meet their individual preferences; and in the use of tools such as recommendation engines that can alert consumers to products and services that might be of interest, based on their search and purchasing histories.
6. The CIGI survey was conducted by Ipsos between December 23, 2016, and March 21, 2017 in 24 economies – Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey and the United States – and involved 24,225 Internet users (CIGI, 2017). Further information can be found at [www.cigionline.org/internet-survey](http://www.cigionline.org/internet-survey).
7. The survey was carried out online between September and October 2016 across 23 countries, including all 19 G20 economies. Further information on the methodology can be found at <http://bit.ly/2HhKOZ1>.
8. See [www.easaalliance.org](http://www.easaalliance.org).
9. See [www.iab.com/news/self-regulatory-principles-for-onlinebehavioral-advertising/](http://www.iab.com/news/self-regulatory-principles-for-onlinebehavioral-advertising/).
10. See [www.ucepcol.com/conared](http://www.ucepcol.com/conared).
11. The standard way of categorising goods or attributes (see OECD, 2010a) draws distinctions between:
  - Search goods: whose attributes and qualities can be observed or verified pre-purchase, for example, the colour of an item of apparel.
  - Experience goods: whose attributes or qualities can only be observed after use. To continue with the apparel example, the durability of item of clothing may fit into this category.
  - Credence goods: whose attributes or qualities cannot be determined by the purchaser even after purchase and use. For example, a single consumer cannot determine, based on personal experience, whether a vitamin supplement that claims to reduce cancer risk actually does so.
12. It is not clear whether reading or understanding terms and conditions would have always solved these issues. For example, delivery issues may be outside of the online terms and conditions. In addition, in many cases the harm could not have been foreseen by the consumer and it may only be after the fact that a consumer knows that they have made the wrong decision. Further, even if a consumer reads and understands the terms and conditions, and does not like them, they might have no choice but to go along with them anyway (OECD, 2018c).
13. See Office of Consumer Affairs’ (Government of Canada), Internet Sales Contract Harmonization Template, <https://bit.ly/2I4eklu>.
14. For example, the FTC’s Dot Com Disclosures guidance, which was updated in 2013. See <https://bit.ly/2an7WX8>
15. It should be noted that, at the time, Microsoft was promoting its Windows Phone software and a child-safe feature to keep children away from apps that could make purchases (see Trenholm, 2013).
16. The OECD peer platform markets survey covered 10 OECD countries, of which 8 – Australia, Canada, Germany, Italy, Japan, Mexico, Turkey and the United States – are G20 economies.
17. For more information, see <http://bit.ly/2Ht7q9e> (English language version).
18. RAPEX facilitates the rapid exchange of information between the national authorities of 31 countries and the European Commission on dangerous products found on the market. It is available at <http://bit.ly/2wAijk5>.
19. The OECD portal is available at <https://globalrecalls.oecd.org/front/index.html#/recalls>.
20. See <https://www.sites.oas.org/rcss/en/pages/default.aspx>



21. See [www.aseanconsumer.org/accp/index.php?r=portal/article&id=3](http://www.aseanconsumer.org/accp/index.php?r=portal/article&id=3).
22. See [pages.ebay.co.uk/help/policies/recalled.html](http://pages.ebay.co.uk/help/policies/recalled.html).
23. This should be seen in the context of respondents completing an average of around 20 transactions in PPMs per year.
24. The analysis was undertaken to support a review of the 2003 *OECD Recommendation on Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders* (OECD, 2003); and to inform work on implementation of the 2016 *Consumer Protection in E-commerce: OECD Recommendation* (OECD, 2016a), specifically the updated section on enforcement co-operation.
25. For example, the KCA's English language complaint form. See <https://bit.ly/2lt0rkU>.
26. However, respondents to the OECD survey indicated considerable differences in conditions for such consumer protection enforcement co-operation. For some countries, it depends on the place where the business conduct occurs. For other countries, the existence of domestic consumers affected by businesses operating in the country seems to be key to enforcement co-operation action against these businesses.
27. The ACCC's Digital Platforms Inquiry is looking at is looking at the impact of digital platforms on the supply of news and journalistic content and the implications of this for media content creators, advertisers and consumers. See <https://bit.ly/2rgTl90>
28. See [www.choice.com.au](http://www.choice.com.au).
29. Annex 3.A1 of the *OECD Consumer Policy Toolkit* (OECD, 2010a) describes approaches to measuring different types of detriment, and summarises some of the key issues that need to be addressed. Further information on techniques that can be employed are described and evaluated in a report undertaken for the European Commission. The report, which was prepared by Europe Economics in 2007, strongly endorses the use of consumer surveys to facilitate measurement (Europe Economics, 2007).
30. For example, the Midata initiative in the United Kingdom. See <https://bit.ly/2hkNYBN>
31. For examples of materials produced by Stay Smart Online for Consumer Fraud Awareness Week, see <https://bit.ly/2umaqlQ>.
32. See [www.consumer.ftc.gov/features/feature-0038-onguardonline](http://www.consumer.ftc.gov/features/feature-0038-onguardonline).

[www.oecd.org/sti/consumer](http://www.oecd.org/sti/consumer)

[www.oecd.org/going-digital](http://www.oecd.org/going-digital)

<http://oe.cd/digital-economy-papers>

 [@OECDInnovation](https://twitter.com/OECDInnovation)